

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-161162

(43)Date of publication of application : 18.06.1999

(51)Int.Cl.

G09C 1/00

G09C 5/00

H04L 9/06

(21)Application number : 09-326455

(71)Applicant : HITACHI LTD

(22)Date of filing : 27.11.1997

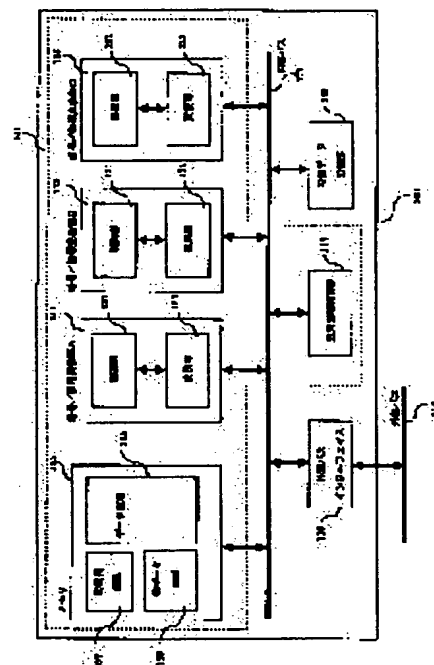
(72)Inventor : AIKAWA SHIN
TAKARAGI KAZUO
FURUYA SOICHI
HIRAHATA SHIGERU

(54) CIPHERING METHOD OR DECIPHERING METHOD, AND DEVICE USING THE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To increase the processing speed of conversion in CBC mode by simultaneously encoding conversion and decoding conversion for blocks taken out of frames wherein a message is divided, one by one.

SOLUTION: In a data area 135, data as objects of ciphering or deciphering conversion are written in order from outside a ciphering/deciphering conversion system 101 and then divided into frames. The frames are each a bit sequence which is longer than the block length as the basis conversion unit of block ciphering conversion. The data written in the data area 135 are read in ciphering/deciphering conversion parts A111 to C113 in parallel and ciphered or deciphered, and the results are written in the data area again. Consequently, the data in the data area 135 are ciphered or deciphered. The data in the data area 135 after the ciphering or deciphering conversion are read sequentially out of the ciphering/deciphering conversion system 101.



LEGAL STATUS

[Date of request for examination]

19.01.2001

[Date of sending the examiner's decision of rejection]

13.07.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C): 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-161162

(43) 公開日 平成11年(1999) 6月18日

(51) Int.Cl.⁶

識別記号

F I

G 0 9 C 1/00

6 1 0

G 0 9 C 1/00

6 1 0 A

5/00

5/00

H 0 4 L 9/06

H 0 4 L 9/00

6 1 1 Z

審査請求 未請求 請求項の数19 O L (全 31 頁)

(21) 出願番号

特願平9-326455

(22) 出願日

平成9年(1997)11月27日

(71) 出願人

000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者

相川 慎

神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所マルチメディアシステム開発本部内

(72) 発明者

宝木 和夫

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74) 代理人

弁理士 小川 勝男

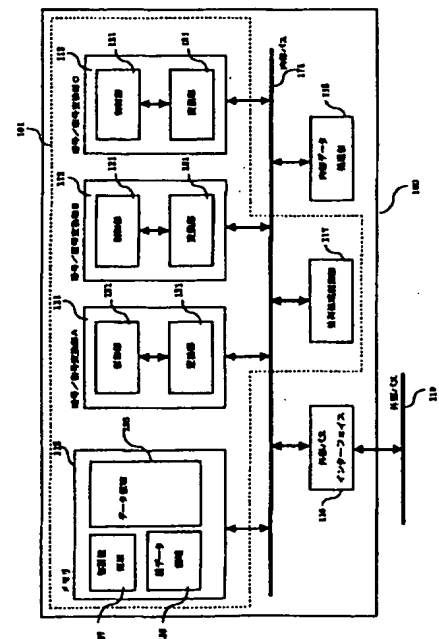
最終頁に続く

(54) 【発明の名称】 暗号化方法または復号化方法およびそれを用いた装置

(57) 【要約】

【課題】 データの暗号変換および復号変換を並列に処理することができる、暗号／復号変換システムを提供すること。

【解決手段】 暗号および復号変換を行う情報処理機器に、複数の演算を並列に行う、複数の演算手段を備え、暗号変換すべき平文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割し、複数フレームから1ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、暗号変換および復号変換を行う構成にする。



【特許請求の範囲】

【請求項1】複数の演算を並列に行う、複数の演算手段と、
暗号変換すべき平文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割する手段と、
複数フレームから1ブロックずつデータを取り出して、取り出した複数ブロックを、前記複数の演算手段に、並列に入力する手段とを備えることを特徴とする並列暗号化装置。

【請求項2】複数の演算を並列に行う、複数の演算手段を用い、
暗号変換すべき平文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割し、
複数フレームから1ブロックずつデータを取り出して、取り出した複数ブロックを、並列に、暗号変換する処理を行うことを特徴とする並列暗号化方法。

【請求項3】複数の演算を並列に行う、複数の演算手段と、
復号変換すべき暗号文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割する手段と、
複数フレームから1ブロックずつデータを取り出して、取り出した複数ブロックを、前記複数の演算手段に、並列に入力する手段とを備えることを特徴とする並列復号化装置。

【請求項4】複数の演算を並列に行う、複数の演算手段を用い、
復号変換すべき暗号文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割し、
複数フレームから1ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、復号変換する処理を行うことを特徴とする並列復号化方法。

【請求項5】複数の演算を並列に行う、複数の演算手段と、
暗号変換すべき平文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割する手段と複数フレームから1ブロックずつデータを取り出して、取り出した複数ブロックを、前記複数の演算手段に、並列に入力する手段と、
復号変換すべき暗号文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割する手段と、
複数フレームから1ブロックずつデータを取り出して、取り出した複数ブロックを、前記複数の演算手段に、並列に入力する手段とを備えることを特徴とする並列暗号化／復号化装置。

【請求項6】複数の演算を並列に行う、複数の演算手段を用い、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割し、
複数フレームから1ブロックずつデータを取り出して、取り出した複数ブロックを、並列に、暗号変換する処理を行い、

復号変換すべき暗号文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割し、
複数フレームから1ブロックずつデータを取り出して、取り出した複数ブロックを、並列に、復号変換する処理を行うことを特徴とする並列暗号化／復号化方法。

【請求項7】複数の演算を並列に行う、2個以上のN個の演算手段を含む暗号変換装置であって、
暗号変換すべき平文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割し、一つのフレームから2乃至N個のブロックを取り出して、取り出した2乃至N個のブロックを、同時に、該暗号変換装置に入力することを特徴とする並列暗号方法および装置。

【請求項8】複数の演算を並列に行う、2個以上のN個の演算手段を含むコンピューターの制御方式であって、
暗号変換すべき平文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割し、一つのフレームから2乃至N個のブロックを取り出して、取り出した2乃至N個のブロックを、同時に、暗号変換する処理を含むことを特徴とする並列暗号方法および装置。

【請求項9】複数の演算を並列に行う、2個以上のN個の演算手段を含む復号変換装置であって、
復号変換すべき平文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割し、一つのフレームから2乃至N個のブロックを取り出して、取り出した2乃至N個のブロックを、同時に、該復号変換装置に入力することを特徴とする並列復号方法および装置。

【請求項10】複数の演算を並列に行う、2個以上のN個の演算手段を含むコンピューターの制御方式であって、
復号変換すべき平文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割し、一つのフレームから2乃至N個のブロックを取り出して、取り出した2乃至N個のブロックを、同時に、復号変換する処理を含むことを特徴とする並列復号方法および装置。

【請求項11】複数の演算を並列に行う、2個以上のN個の演算手段を含む暗号／復号変換装置であって、
暗号変換すべき平文メッセージを、ブロック暗号の基本

単位である 1 ブロック長よりも長い、ビット列を 1 フレームとする、複数フレームに分割し、一つのフレームから 2 乃至 N 個のブロックを取り出して、取り出した 2 乃至 N 個のブロックを、同時に、該暗号／復号変換装置に入力する、並列暗号方法、および、復号変換すべき平文メッセージを、ブロック暗号の基本単位である 1 ブロック長よりも長い、ビット列を 1 フレームとする、複数フレームに分割し、一つのフレームから 2 乃至 N 個のブロックを取り出して、取り出した 2 乃至 N 個のブロックを、同時に、該暗号／復号変換装置に入力する、並列復号方法、を用いることを特徴とする並列暗号／復号方法および装置。

【請求項 1 2】複数の演算を並列に行う、2 個以上の N 個の演算手段を含むコンピューターの制御方式であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である 1 ブロック長よりも長い、ビット列を 1 フレームとする、複数フレームに分割し、一つのフレームから 2 乃至 N 個のブロックを取り出して、取り出した 2 乃至 N 個のブロックを、同時に、暗号変換する、並列暗号方法、および、復号変換すべき平文メッセージを、ブロック暗号の基本単位である 1 ブロック長よりも長い、ビット列を 1 フレームとする、複数フレームに分割し、一つのフレームから 2 乃至 N 個のブロックを取り出して、取り出した 2 乃至 N 個のブロックを、同時に、復号変換する、並列復号方法、を用いる処理を含むことを特徴とする並列暗号／復号方法および装置。

【請求項 1 3】複数の演算を並列に行う、複数の演算手段を含む暗号変換装置であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である 1 ブロック長よりも長い、ビット列を 1 フレームとする、複数フレームに分割し、複数フレームから 1 ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、該暗号変換装置に入力し、複数の暗号文ブロックを出力し、該複数の暗号文ブロックを、再度、該暗号変換装置に入力することを特徴とする並列暗号方法および装置。

【請求項 1 4】複数の演算を並列に行う、複数の演算手段を含むコンピューターの制御方式であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である 1 ブロック長よりも長い、ビット列を 1 フレームとする、複数フレームに分割し、複数フレームから 1 ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、暗号変換し、複数の暗号文ブロックを出力し、該複数の暗号文ブロックを、次に暗号変換する、複数の平文ブロックの暗号変換に用いる処理を含むことを特徴とする並列暗号方法および装置。

【請求項 1 5】複数の演算を並列に行う、複数の演算手段を含む暗号変換装置であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本

単位である 1 ブロック長よりも長い、ビット列を 1 フレームとする、複数フレームに分割し、複数フレームから 1 ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、該暗号変換装置に入力し、各複数ブロックに対して、暗号変換を行い、各暗号変換途中に得られる、複数の中間ブロックを、再度、暗号変換装置に入力することを特徴とする並列暗号方法および装置。

【請求項 1 6】複数の演算を並列に行う、複数の演算手段を含むコンピューターの制御方式であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である 1 ブロック長よりも長い、ビット列を 1 フレームとする、複数フレームに分割し、複数フレームから 1 ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、暗号変換し、各暗号変換途中に得られる、複数の中間ブロックを、次に暗号変換する、複数の平文ブロックの暗号変換に用いる処理を含むことを特徴とする並列暗号方法および装置。

【請求項 1 7】装置 A と装置 B と装置 C は、お互いに暗号通信できるように構成されており、前記装置 A または前記装置 B から前記装置 C に送信されたデータは、暗号変換されないままであるかどうかを前記装置 C が検査する手段と、該データが暗号変換されないままであることが検知された場合には、そのことを示す信号を別の装置 D に送信する手段とを備えることを特徴とする暗号通信システム。

【請求項 1 8】前記装置 D は、前記データが暗号変換されないままであることが検知されたことを示す信号を受信した場合、前記装置 D から前記装置 A または前記装置 B に送信するデータを制限する手段を有することを特徴とする請求項 1 7 記載の暗号通信システム。

【請求項 1 9】前記装置 A または B は装置 E と通信できるように構成されており、前記装置 E は前記装置 A に平文データを暗号方式 1 により暗号化した暗号文 1 を送る手段を備え、前記装置 A は該暗号文 1 を該暗号方式 1 に対応する復号方式 1 により復号する手段と、もとの平文データを得た後、暗号方式 1 とは異なる暗号方式 2 で平文データを再暗号化して暗号文 2 を得た後、前記装置 B に暗号文 2 を送信する手段とを備えることを特徴とする請求項 1 7 記載の暗号通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータ、情報処理装置、情報家電機器等の間で伝送されるデータの、暗号／復号技術に関するものである。

【0002】

【従来の技術】近年の、パーソナルコンピュータや、デジタル情報家電の普及に伴い、画像、音声、データなどのマルチメディア情報を機器間でやり取りする機会が増えてきた。マルチメディア・データは、デジタル・デー

タなので、簡単に複製できてしまい、不正コピーや、著作権侵害などが、大きな問題となっている。この問題を解決するには、暗号技術が必須となる。機器間を接続する通信路上を流れるデータを暗号化することで、盗聴および改ざんを防止し、不正コピーを防ぐことができる。データの暗号化に関しては、ブロック暗号を用いる場合が多い。

【0003】ブロック暗号とは暗号化したいデータを一定長のデータ（ブロックデータ）に分割し、ブロック単位に、同一長の暗号データに暗号化する共通鍵暗合方式である。ブロック暗号においては、通常一定の期間に同一の暗号鍵が使用されるため、同一のブロックデータがいつも同一の暗号データに変換されることになり、安全上あまり望ましくない。そこで、その対処法として、ブロック暗号の利用モードのある暗号文ブロック連鎖（Cipher Block Chaining, CBC）モードを用いることが多い。以下、CBCモードによる暗号変換および復号変換方式についての説明を図24を用いて行う。ここで、ブロックデータの長さは64ビットとして説明していく。図24において、2001から2003はブロック暗号変換部であり、2011から2013はブロック復号変換部である。すべてのブロック暗号部およびブロック復号部は、同じ鍵データを用いる。また、2021から2026は排他的論理和演算部である。

【0004】まず、CBCモードによる暗号変換について説明する。暗号化したいデータ（平文データ）は、先頭から、64ビット長のブロックデータに分割されていく。これを平文ブロックと呼ぶ。図24においては、平文データは、平文ブロックM[1]241、平文ブロックM[2]242、平文ブロックM[3]243、... というように分割されていく。平文ブロックは、暗号変換され、暗号文ブロックとなる。最初の平文ブロックM[1]241の暗号変換には、64ビット長の初期値IV2061を用いる。M[1]241と初期値IV2061は排他的論理和部2021で、排他的論理和をとった後に、ブロック暗号部2001で暗号変換されて、暗号文ブロックC[1]251になる。次に、平文ブロックM[2]242は、暗号文ブロックC[1]251と排他的論理和部2022で、排他的論理和をとった後に、ブロック暗号部2002に入力され、暗号化されて、暗号文ブロックC[2]252になる。以下、同様の処理を、繰り返して、暗号文ブロックを生成していく。変換された、暗号文ブロックを順番に結合したものが、暗号文データになる。以上が、CBCモードによる暗号変換である。CBCモードによる暗号変換は、直前に変換した暗号文ブロックを、順次、フィードバックしていくので、最初の平文ブロックから順番に変換していく必要がある。

【0005】次に、CBCモードによる復号変換について説明する。前述したCBCモードによる暗号変換で、暗号変換された、暗号文データは、暗号文ブロックC[1]251、暗号文ブロックC[2]252、平文ブロックC[3]25

3、... というように分割されていく。最初の暗号文ブロックC[1]251の暗号変換には、64ビット長の初期値IV2061を用いる。これは、前述の暗号変換の際に用いた初期値と同じ値である。C[1]251は、ブロック復号部2011で復号変換して、初期値IV2061と、排他的論理和部2024で、排他的論理和をとって、平文ブロックM[1]241になる。

【0006】次に、暗号文ブロックC[2]252は、ブロック復号部2012で復号変換して、暗号文ブロックC[1]251と排他的論理和部2025で、排他的論理和をとって、平文ブロックM[2]242になる。以下、同様の処理を、繰り返して、平文ブロックを生成していく。生成された、平文ブロックを順番に結合したものが、平文データになる。以上が、CBCモードによる復号変換である。CBCモードによる復号変換は、前述したCBCモードの暗号変換とは異なり、変換結果は、フィードバックされない。

【0007】

【発明が解決しようとする課題】前述したように、CBCモードによる暗号変換は、最初のブロックデータから順番に処理していく必要があるので、高速処理の妨げとなっていた。

【0008】本発明の目的は、CBCモードによる暗号変換および復号変換の処理速度を向上させることにあ

る。

【0009】より具体的には、データの暗号変換および復号変換を並列化する手段を提供し、暗号変換および復号変換の処理速度を向上させることにあ

【0010】

【課題を解決するための手段】上述した目的を達成するため、暗号および復号変換を行う情報処理機器は、複数の演算を並列に行う、複数の演算手段を備え、暗号変換すべき平文メッセージを、ブロック暗号の基本単位である1ブロック長よりも長い、ビット列を1フレームとする、複数フレームに分割し、複数フレームから1ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、暗号変換および復号変換を行う。

【0011】

【発明の実施の形態】以下、本発明の実施の形態を、図面を用いて説明する。

【0012】図1は、本発明の第1実施形態に係る、暗号／復号変換システムを内蔵した、情報処理機器の構成図である。図1において、100は情報処理機器、119は外部バスである。また、情報処理機器100は、暗号／復号変換システム101と、外部バスインターフェイス116と、内部データ処理部118が、内部バス171で接続された形態で構成されている。情報処理機器100は、外部バス119を介して、他の機器から暗号文データを受け取り、暗号／復号変換システム101で、復号化して、平文データを得て、内部データ処理部118でデータ処理をする機能と、内部データ処理部118から、出力される平文データを、

暗号／復号変換システム101で、暗号化して、暗号文データを得て、外部バス119を介して、他の機器に送信する機能を持っている。このような情報処理機器100の具体例として、たとえば、デジタルVTRや、デジタル放送受信機内蔵TVなどが考えられる。

【0013】暗号／復号変換システム101は、暗号／復号変換部A111と、暗号／復号変換部B112と、暗号／復号変換部C113と、メモリ115と、並列処理制御部117とで構成される。

【0014】暗号／復号変換部A111と、暗号／復号変換部B112と、暗号／復号変換部C113は、制御部121と、変換部131で構成される。変換部131は、従来の技術で説明した、CBCモードによる暗号変換および復号変換を行う。

【0015】メモリ115には、データ領域135と、鍵データ領域136と、初期値領域137に分割される。データ領域135は、暗号／復号変換するデータを一時的に保存する領域である。鍵データ領域136は、暗号／復号変換に用いる、鍵データを保存する領域である。初期値領域137は、CBCモードにおける、暗号／復号変換の際に用いる初期値を保存しておく領域である。ここで、鍵データおよび初期値は、暗号通信を行いたい機器間で、共有しておく必要がある。本発明においては、機器間での鍵共有については直接関係しないので詳細は省略することにする。

【0016】データ領域135には、暗号／復号変換システム101外部から、暗号あるいは復号変換を行いたいデータが、順次、書き込まれてくる。データ領域135に書き込まれてくるデータは、暗号／復号変換部A111と、暗号／復号変換部B112と、暗号／復号変換部C113に、並列に読み込まれていき、暗号あるいは復号変換され、その結果が再び、データ領域に書き込まれていく。これによって、データ領域135内のデータが暗号あるいは復号変換処理されていく。データ領域135内の暗号あるいは復号変換処理されたデータは、順次、暗号／復号変換システム101外部に読み出されていく。

【0017】以下、暗号／復号変換システム101が、平文データを暗号変換する手順を図2を用いて説明していく。平文データ220は、データ領域135に書き込まれ、暗号変換を行うために、フレームに分割されていく。ここで、フレームは、ブロック暗号変換の基本変換単位であるブロック長よりも、長いビット列である。CBCモードにおける暗号変換は、フレーム毎に完結するものとする。これによって、各フレームの暗号変換は、鍵データと初期値が与えられれば、独立に行うことができる。CBCモードにおける暗号変換は、従来の技術で説明したように、ブロック単位に行われるので、データ領域135に書き込まれたフレームは、ブロックに区切られる。ここで、ブロック長は64ビットとする。

【0018】図2においては、平文フレームA221は、

平文ブロックM[1]241、平文ブロックM[2]242、平文ブロックM[3]243、... 平文ブロックM[n]248とn個のブロックに分割される。ここで、最後の平文ブロックM[n]248の長さが、64ビット未満の場合は、端数平文ブロックとして区別しておく。同様に、データ領域135内の他の平文フレームもブロックに区切られていく。ブロックに分割された、平文フレームA221は、暗号／復号変換部A111において、ブロック単位に、データ領域135から読み出され、CBCモードを用いて暗号変換されて、再びデータ領域135の同じ場所に書き込まれていく。すなわち、平文ブロックM[1]241は暗号文ブロックC[1]251に変換され、平文ブロックM[2]242は暗号文ブロックC[2]252に変換され、... というように、順次ブロック列を暗号変換していく。ここで、最後の平文ブロックが端数平文ブロックの場合は、CBCモードとは異なる方法を用いて、暗号変換する。これを端数処理と呼ぶ。詳細は後述する。暗号／復号変換部111で暗号変換された、暗号文ブロックC[1]251、暗号文ブロックC[2]252、暗号文ブロックC[3]253、... 暗号文ブロックC[n]258、は、暗号文フレームA231として、結合される。

【0019】同様な処理を、平文フレームBについては暗号／復号変換部B112が、暗号文フレームB232に変換し、平文フレームC223については暗号／復号変換部C113が、暗号文フレームC233に変換していく。これによって、平文フレームの暗号変換を、並列に行っていくことができる。ここで、それぞれの暗号／復号変換部は、変換の前に、鍵データ領域136から鍵データを、初期値領域137から初期値データを読み込んでおく必要がある。この並列処理の制御は、並列処理制御部117が行い、それぞれの暗号／復号変換部が、平文データのどのフレームを暗号変換すればよいかを指示していく。

【0020】以上、平文データを複数の暗号／復号変換部で暗号変換していく方法について説明したが、同様に、暗号文データを複数の暗号／復号変換部で復号変換していく手順について、図3を用いて説明する。

【0021】暗号文データ230は、データ領域135に書き込まれ、復号変換を行うために、フレームに分割されていく。前述の暗号変換で説明したのと同様に、それぞれのフレームは、さらに、下位構造であるブロックに区切られ、暗号／復号変換部は、順次、暗号文ブロック列を読み込んで、CBCモードを用いて、平文ブロックに復号変換して、再びデータ領域135の同じ場所に書き込んでいく。ここで、最後の暗号文ブロックの長さが、64ビット未満の場合は、端数暗号文ブロックとして区別し、端数処理によって、復号変換を行う。詳細は後述する。復号変換された、平文ブロック列は、平文フレームとして結合される。CBCモードによる復号変換は、フレーム毎に完結するので、複数の暗号／復号変換部を用いて、暗号文フレームを、並列に、復号変換していくことが可能である。この並列処理の制御は、並列処理制御

部117が行い、それぞれの暗号／復号変換部が、暗号文データのどのフレームを復号変換すればよいかを指示していく。

【0022】次に、図1における、変換部131の内部構造について、詳細に説明する。

【0023】図4は、変換部131の詳細構成図であり、以下のモジュールより構成される。411と412と414は3入力マルチプレクサ、413と415は2入力マルチプレクサ、421と422はレジスタ、431は排他的論理和演算部、441はブロック暗号部である。上記モジュールの入力および出力は、すべて64ビットのバラレル入出力である。ブロック暗号部441は、従来の技術で説明したように、ブロック暗号方式による暗号変換および復号変換を行う。ブロック暗号方式は、通常、暗号変換と復号変換のアルゴリズムが、よく似ているので、容易に、暗号変換と復号変換を共有できるブロック暗号器を設計することができる（たとえば、本発明者によって提案されている（特願平09-213327）に詳しい）。

【0024】初めに、この変換部131がCBCモードによる暗号変換を行う手順について説明する。変換部131には、平文ブロック列が順次入力され、暗号文ブロックを順次出力していく。一番目の平文ブロックの変換のときだけは、マルチプレクサ414を介して、レジスタ422に初期値を設定して保持しておく。平文ブロックは、マルチプレクサ411を介して、排他的論理和演算部431に入力され、一方、レジスタ422の値は、マルチプレクサ415を介して、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値は、マルチプレクサ412を介して、ブロック暗号部441に入力され、鍵データを用いて、暗号化される。ここで、ブロック暗号部441は暗号モードに設定する。ブロック暗号部441からの出力は、暗号文ブロックとして、出力されるとともに、次の平文ブロックへのフィードバック値として、マルチプレクサ414を介して、レジスタ422の値を更新し保持される。以上の様な変換を繰り返していくことで、平文ブロックを、暗号文ブロックに順次変換していく。ここで、最後の平文ブロックが、端数平文ブロックの場合は、以下のように端数処理を行って、端数暗号文ブロックに変換する。

【0025】端数平文ブロックは、マルチプレクサ411を介して排他的論理和演算部431に入力され、一方で、レジスタ422の値（直前の暗号文ブロック）を、マルチプレクサ415および412を介して、ブロック暗号部441で暗号変換し（このとき暗号モードに設定する）、出力結果を、マルチプレクサ413と415を介して、排他的論理和演算部431に入力する。排他的論理和演算部431の出力値はマルチプレクサ413を介して、端数暗号文ブロックとして、出力される。

【0026】以上の処理によって、変換部131は、平文ブロック列を、暗号文ブロック列に暗号変換していくこ

とができる。ここで、マルチプレクサのスイッチング、レジスタの値の保存と書き換え、ブロック暗号部の暗号モードの設定は、制御部121が行う。

【0027】次に、この変換部131がCBCモードによる復号変換を行う手順について説明する。変換部131には、暗号文ブロック列が順次入力され、平文ブロックを順次出力していく。一番目の暗号文ブロックの変換のときだけは、マルチプレクサ414を介して、レジスタ422に初期値を設定して保持しておく。暗号文ブロックは、レジスタ421に保持されるとともに、マルチプレクサ412を介して、ブロック暗号部441に入力されて、復号化される。ここで、ブロック暗号部441は復号モードに設定する。ブロック暗号部441の出力値はマルチプレクサ411を介し、排他的論理和演算部431に入力され、一方で、レジスタ422の値は、マルチプレクサ415を介して、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値はマルチプレクサ413を介して、平文ブロックとして、出力される。この時、レジスタ421に保持されていた値を、マルチプレクサ414を介して、レジスタ422に保持する。以上の様な変換を繰り返していくことで、文ブロックを、暗号文ブロックに順次変換していく。ここで、最後の暗号文ブロックが、端数暗号文ブロックの場合は、以下のように端数処理を行って、端数平文ブロックに変換する。

【0028】端数暗号文ブロックは、マルチプレクサ411を介して排他的論理和演算部431に入力され、一方で、レジスタ422の値を、マルチプレクサ412を介して、ブロック暗号部441で暗号変換し（このとき暗号モードに設定する）、出力結果を、マルチプレクサ413と415を介して、排他的論理和演算部431に入力する。排他的論理和演算部431の出力はマルチプレクサ413を介して、端数平文ブロックとして、出力される。

【0029】以上の処理によって、変換部131は、暗号文ブロック列を、平文ブロック列に復号変換していくことができる。ここで、マルチプレクサのスイッチング、レジスタの値の保存と書き換え、ブロック暗号部441の暗号および復号モードの設定は、制御部121が行う。

【0030】以上より、変換部131は、暗号変換および復号変換の両方を行うことが可能である。

【0031】前述したように、暗号／復号変換システム101は、複数の暗号／復号変換部を用いて、CBCモードによる暗号変換、あるいは復号変換を、並列に行うことができ、一つの暗号／復号変換部のみを用いた場合よりも、より高速に暗号／復号変換を行うことができる。この暗号／復号変換システム101は、複数の暗号文データおよび平文データを、同時に、暗号／復号変換することも可能である。たとえば、図5において、暗号／復号変換システム101は、内部データ処理部118から出力される平文データA511を、暗号変換すると同時に、外部バスインターフェイス116が、外部バス119から受信

する暗号文データB521を、復号変換している。ここで、平文データAおよび暗号文データBは、リアルタイム・データであるとし、平文データAの方が、暗号文データBより、ビットレートが大きいものとする。また、暗号／復号変換部A111と、暗号／復号変換部B112と、暗号／復号変換部C113の暗号変換および復号変換の処理速度は、すべて同じであるとし、単独では、暗号文データBは、リアルタイムで復号変換できるが、平文データAの暗号変換は、不可能であるとする。しかし、2つの暗号／復号変換部を並列化して用いて、処理速度を2倍にすれば、平文データAを、リアルタイムに暗号変換できるものとする。

【0032】この場合、平文データAはデータ領域135に書き込まれていき、暗号／復号変換部A111と、暗号／復号変換部B112で、並列に暗号変換されていく。この並列暗号変換方法は前述した通りである。また、暗号文データB135も同時に、データ領域135に書き込まれていき、暗号／復号変換部C113で、復号変換されていく。また、鍵データ領域136には、平文データAの暗号化に用いる鍵データA512と、暗号文データBの復号化に用いる、鍵データB513が保存されており、初期値領域137には、平文データAの暗号化に用いる初期値A522と、暗号文データBの復号化に用いる、初期値B523が保存されている。平文データA511を暗号変換するために、事前に、鍵データA512と初期値A522を、暗号／復号変換部A111と、暗号／復号変換部B112に設定し、暗号文データB521を復号変換するために、鍵データB513と初期値B523を、暗号／復号変換部C113に設定しておく。これによって、二つの、データの暗号変換および復号変換を、同時にリアルタイムで行うことが可能になる。

【0033】次に、暗号／復号変換システム101を用いて、複数のリアルタイム・データを暗号／復号変換するための、暗号／復号変換部の管理方法について述べる。暗号／復号変換システム101を用いてリアルタイム・データの暗号変換および復号変換を行う場合、それぞれのリアルタイム・データのビットレートに合せて、使用する暗号／復号変換部の数を動的に設定することができる。これによって、効率的に、暗号／復号変換部を使用することができる。以下、この管理方法について、図面を用いて説明していく。ここで、以下の説明において、暗号／復号変換システム101内にはN個の暗号／復号変換部が並列化されているものとして一般化する。また、それぞれの暗号／復号変換部の処理速度をA[bps]とする。また、暗号／復号変換システム101の並列処理制御部117は、図6に示すような変換部管理情報330を保持している。変換部管理情報330は、未使用の暗号／復号変換部の数M331と、管理変数n332と、管理テーブル340から構成される。管理テーブル340は、それぞれの暗号／復号変換部の、識別番号341と、変換するリアルタ

イム・データの識別番号342と、暗号／復号変換部の変換モード343と、使用状態344から成る。

【0034】図7は、暗号／復号変換システム101の並列処理制御部117が行う、暗号／復号変換部の管理手順を示したフローチャートである。このフローチャートを元に、管理手順をステップ毎に説明していく。

【0035】まず初めに、ステップ301で管理テーブルが初期化される。すなわち、すべての暗号／復号変換部の使用状態344を「未使用」にする。次に、ステップ302で未使用の暗号／復号変換部の数M331に、全暗号／復号変換部数Nを代入する。

【0036】次に、ステップ303で並列暗号／復号変換システムに入力される、リアルタイム・データの増減を監視する。

【0037】まず、ステップ303で、リアルタイム・データが新たに増えた場合を説明する。この場合、まず、ステップ305でこのリアルタイム・データを処理するために使用する暗号／復号変換部の数を計算して、管理変数n332に代入する。新たに入力されるリアルタイム・データのビットレートをB[bps]とすれば、暗号／復号変換部の数mは、以下の不等式

$$B < mA$$

を満たさなければ、リアルタイムに暗号／復号変換を行うことができない。そこで、ステップ304では、使用する暗号／復号変換部の数を $[B/A]$ と定め、管理変数n332に代入する。ここで、 $[B/A]$ は、BをAで割った結果の少数部を切り上げて整数化する演算を表す。次に、ステップ305で現在の未使用な暗号／復号変換部の数M331と管理変数n332を比較し、nのほうが小さければ、割当て成功となり、ステップ306で管理テーブル340の変更を行う。これは以下のように処理する。まず、管理テーブル340の使用状態344を検索していき、「未使用」の暗号／復号変換部をn個選び出す。検索方法は、たとえば、暗号／復号変換部の識別番号341の若い順に検索していけばよい。選び出したn個について、識別番号342にリアルタイム・データの識別番号を設定し、リアルタイム・データを暗号変換するならモード343を「暗号」に、復号変換するなら「復号」に設定する。最後に選び出したn個暗号／復号変換部の使用状態344を「使用」に変更する。次に、ステップ306で未使用の暗号／復号変換部の数M331を $M-n$ に更新する。最後に、ステップ311で、更新された管理テーブル340の各項目を元に、並列処理制御部117が、必要な暗号／復号変換部を制御して、リアルタイム・データの暗号／復号変換を開始する。

【0038】前記ステップ305において、もし割当てが失敗したら、ステップ310で適切なエラー処理を行い、再びステップ303に戻る。エラー処理は、たとえば、必要な暗号／復号変換部がすべて、未使用になるまで待機するなどの処理を行う。以上、入力リアルタイム・デー

タが新たに増えた場合の処理について説明した。

【0039】次に、入力リアルタイム・データが減った場合について説明する。この場合は任意のリアルタイム・データの暗号／復号変換が終了した後に、使用していた暗号／復号変換部を開放する処理を行う。まず、ステップ308で管理テーブル340の更新を行う。これは以下のように処理する。まず、管理変数 $n332$ を0に初期化する。次に暗号／復号変換が終了したリアルタイム・データの識別番号を管理テーブル340から、すべて選び出す。この選択方法は、たとえば、暗号／復号変換部の識別番号の若い順に最後まで検索してけばよい。識別番号が見つかった場合、その暗号／復号変換部の使用状態344を「未使用」に変更し、管理変数 $n332$ を1増やす。最後まで検索が終了すると、管理変数 $n332$ には、使用していた暗号／復号変換部の数が入力されていることになる。次に、ステップ309で未使用の暗号／復号変換部の数 $M331$ を $M+n$ に更新し、ステップ303に戻る。以上、入力リアルタイム・データが減った場合の処理について説明した。

【0040】上述した、本発明を用いた実施形態の説明において、暗号／復号変換システム101による、暗号および復号変換は、CBCモードを用いていたが、他の暗号運用モードを用いることも可能である。例えば、ブロック暗号方式をそのまま適用する基本モードである、ECB (Electronic Code Book) モードを用いる場合を考える。この場合、各フレーム内の各ブロックは、独立に処理することができるので、一つのフレームから、ブロックを複数個取り出し、取り出したそれぞれのブロックを、別々の暗号／復号変換器で、同時に変換していく、ということを経り返していくことで、並列処理を行うことができる。

【0041】次に、本発明の他の実施形態を説明する。図8は、本発明の他の実施形態に係る、復号変換システムを内蔵した、情報処理機器の構成図である。情報処理機器800は、前記第1実施形態の情報処理機器100と同様の、外部バスインターフェイス116と、内部データ処理部118とに加えて、復号変換システム801が、内部バス171で接続された形態で構成されている。情報処理機器800は、外部バス119を介して、他の機器から暗号文データを受け取り、復号変換システム801で、復号化して、平文データを得て、内部データ処理部118でデータ処理をする機能を持っている。情報処理機器800は、機器内部で復号変換しか行わないので、復号変換システム801は、本発明の第1実施形態の暗号／復号変換システム101よりも、簡単な構成で実現できる。ような情報処理機器800の具体例として、たとえば、デジタルTVなどが考えられる。

【0042】本実施形態においても、データの復号変換にCBCモードを用いるとすれば、本発明の第1実施形態で説明したように、暗号／復号変換システム101で

は、フレーム単位でしか並列処理が行えなかったのに対して、復号変換システム801は、復号変換のみ行えばよいので、ブロック単位に並列処理を行うことができ、暗号／復号変換システム101に比べて、少ないメモリ容量で、並列処理できる。

【0043】復号変換システム801は、第1実施形態の暗号／復号変換システム101と同様に、メモリ115に加えて、復号変換部A811と、復号変換部B812と、復号変換部C813と、メモリ115と、並列処理制御部817とで構成される。

【0044】復号変換部A811と、復号変換部B812と、復号変換部C813は、制御部821と、変換部831で構成される。変換部831は、従来の技術で説明した、CBCモードによる復号変換を行う。

【0045】以下、暗号／復号変換システム801が、暗号文データを復号変換する手順を図9を用いて説明していく。暗号文データ230は、データ領域135に書き込まれていき、CBCモードで復号変換を行うために、フレームに分割され、さらに各フレームは、ブロックに分割される。ここで、ブロック長は64ビットとする。従来の技術で説明したように、CBCモードにおける、暗号文ブロックの復号変換は、直前の暗号文ブロックを用いるだけでよいので、暗号変換のように、変換したブロックを、フィードバックする必要がない。したがって、同一フレーム内でも、直前の暗号文ブロックを参照できれば、ブロック単位に独立に復号変換を行うことができる。

【0046】図9においては、暗号文データは、暗号文フレームA231、暗号文フレームB232、暗号文フレームC233、...というようにフレーム分割される。暗号文フレームA231は、暗号文ブロックC[1]251、暗号文ブロックC[2]252、暗号文ブロックC[3]253、...暗号文ブロックC[n]258とn個のブロックに分割される。ここで、最後の暗号文ブロックC[n]258の長さが、64ビット未満の場合は、端数暗号文ブロックとして区別しておく。暗号ブロックが、順番にデータ領域135に書き込まれていくと、復号変換部A811は、暗号文ブロックC[1]251と、初期値領域から、初期値を読み込み、復号変換して、平文ブロックM[1]をデータ領域135に書き込む。復号変換部B812は、暗号文ブロックC[2]252と、暗号文ブロックC[2]251を読み込み、復号変換して、平文ブロックM[2]をデータ領域135に書き込む。同様に、復号変換部C812は、暗号文ブロックC[3]253と、暗号文ブロックC[2]252を読み込み、復号変換して、平文ブロックM[3]をデータ領域135に書き込む。以上のような暗号ブロックの復号化を、復号変換部A811と、復号変換部B812と、復号変換部C813が、最後のブロックまで、並列に処理していく。これによって、同一フレーム内での、並列復号変換を行うことが可能になる。この並列処理の制御は、並列処理制御部817が行い、それぞれの復号変換部が、どの

暗号文ブロックを復号変換すればよいかを指示していく。

【0047】次に、本実施例の変換部831の内部構造について、詳細に説明する。

【0048】図10は、変換部831の詳細構成図であり、以下のモジュールより構成される。1011は2入力マルチプレクサ、1012は3入力マルチプレクサ、431は排他的論理和演算部、441はブロック暗号部である。上記モジュールの入力および出力は、すべて64ビットのパラレル入出力である。ブロック暗号部441は、第1実施形態で説明したものと同様である。

【0049】まず、一番先頭の暗号文ブロックの復号変換を考える。この場合、変換部431には暗号文ブロックC[1]と、初期値と、鍵データが入力される。暗号文C[1]はマルチプレクサ1011を介して、ブロック暗号部441に入力され、鍵データを用いて、復号変換される。ここで、ブロック暗号部441は復号モードに設定する。ブロック暗号部441からの出力は、排他的論理和演算部431に入力される。一方で、初期値がマルチプレクサ1012を介して、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値が、平文ブロックM[1]となる。

【0050】次に、2からn-1の間の任意の整数をkとし、k番目の暗号文ブロックの復号変換を考える。この場合、変換部431には暗号文ブロックC[k]とその直前の暗号文ブロックC[k-1]と、鍵データが入力される。暗号文ブロックC[k]はマルチプレクサ1011を介して、ブロック暗号部441に入力され、鍵データを用いて、復号変換される。ここで、ブロック暗号部441は復号モードに設定する。ブロック暗号部441からの出力は、排他的論理和演算部431に入力される。一方で、暗号文ブロックC[k-1]がマルチプレクサ1012を介して、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値が、平文ブロックM[k]となる。

【0051】次に、n番目すなわち最後の暗号文ブロックの復号変換を考える。この場合、変換部431には、暗号文ブロックC[n]とその直前の暗号文ブロックC[n-1]と、鍵データが入力される。

【0052】まず、暗号文ブロックC[n]が、端数暗号文ブロックである場合は、以下のように端数処理を行う。暗号文ブロックC[n]はマルチプレクサ1012を介して、排他的論理和演算部431に入力される。一方で、暗号文ブロックC[n-1]がマルチプレクサ1011を介して、ブロック暗号部441に入力され、鍵データを用いて、暗号変換される。ここで、ブロック暗号部441は暗号モードに設定する。ブロック暗号部441からの出力は、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値が、平文ブロックM[n]となる。

【0053】次に暗号文ブロックC[n]が、端数ブロックでなければ以下のように変換を行う。暗号文ブロックC[n]はマルチプレクサ1011を介して、ブロック暗号部441

に入力され、鍵データを用いて、復号変換される。ここで、ブロック暗号部441は復号モードに設定する。ブロック暗号部441からの出力は、排他的論理和演算部431に入力される。一方で、暗号文ブロックC[n-1]がマルチプレクサ1012を介して、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値が、平文ブロックM[n]となる。

【0054】以上の処理によって、変換部431は、暗号文ブロック列を、暗号文ブロック列に暗号変換していくことができる。ここで、マルチプレクサのスイッチング、ブロック暗号部の暗号および復号モードの設定は、制御部821が行う。

【0055】上述した実施形態の説明において、復号変換システム801による、復号変換は、CBCモードを用いていたが、他の暗号運用モードを用いることも可能である。例えば、ブロック暗号方式をそのまま適用する基本モードである、ECB(Electronic Code Book)モードを用いる場合を考える。この場合、各フレーム内の各ブロックは、独立に処理することができるので、一つのフレームから、ブロックを複数個取り出し、取り出したそれぞれのブロックを、別々の復号変換器で、同時に変換していく、ということを繰り返していくことで、並列処理を行うことができる。

【0056】次に、本発明の他の実施形態を説明する。図11は、本発明の他の実施形態に係る、暗号/復号変換システムを内蔵した、情報処理機器の構成図である。情報処理機器1100は、前記第1実施形態の情報処理機器100と同様の、外部バスインターフェイス116と、内部データ処理部118とに加えて、暗号/復号変換システム1101が、内部バス171で接続された形態で構成されている。

【0057】暗号/復号変換システム1101は、CPU1101と、メモリ1115とで構成される。CPU1101は、実行部A1111と、実行部B1112と、実行部C1113と、命令部1121と、レジスタ部1130が、内部CPUバス1141で接続されている構成で、3本のパイプラインをもつ、スーパースカラ方式のCPUである。ここで、スーパースカラ方式とは、複数の実行部を備えることで、1クロック・サイクル当たり、複数の独立した命令を同時に実行することができる方式である。

【0058】メモリ1115は、前記第1実施形態のメモリ115と同様の、データ領域135と、鍵データ領域136と、初期値領域137とに加えて、プログラム領域1181に分割される。プログラム領域1181には、CPU1101で暗号/復号変換を行うための、制御プログラムが格納される。

【0059】この制御プログラムは、ROM、Floppy disk、または、ネットワークを介して本システムに接続されたサーバ上の記憶装置から取り込まれることができる。

【0060】レジスタ部1130内には、レジスタA1131と、レジスタB1132と、レジスタC1133が含まれ、それ

ぞれ1個以上のレジスタから構成される、このような、情報処理機器1100の具体例として、パーソナルコンピュータなどが考えられる。

【0061】データ領域135には、暗号／復号変換システム101外部から、暗号あるいは復号変換を行いたいデータが、順次、書き込まれてくる。一方、プログラム領域に格納されている、制御プログラムをCPU1110の命令部1121が、順次読み込んで実行していく。制御プログラムは、データ領域135に書き込まれてくるデータを、レジスタ部1130のレジスタA1131と、レジスタB1132と、レジスタC1133に、読み込んで、実行部A1111と、実行部B1112と、実行部C1113を、並列に用いて、暗号あるいは復号変換させ、その結果を再び、データ領域135に書き込んでいくように、プログラムされている。これによって、データ領域135内のデータが暗号あるいは復号変換処理されていく。データ領域135内の暗号あるいは復号変換処理されたデータは、順次、暗号／復号変換システム1101外部に読み出されていく。

【0062】以下、暗号／復号変換システム1101が、具体的にはCPU1110が制御プログラムを実行し、平文データを暗号変換する手順を図12を用いて説明していく。第1実施例の暗号／復号変換システム101と同様に、平文データ220は、データ領域135に書き込まれ、暗号変換を行うために、フレームに分割され、さらにブロックに区切られていく。次に、平文フレームA221の、先頭の平文ブロックを、レジスタA1131に読み込み、続いて、平文フレームB222の、先頭の平文ブロックを、レジスタB1132に読み込み、続いて、平文フレームC223の、先頭の平文ブロックを、レジスタC1133に読み込む。レジスタA1131およびレジスタB1132およびレジスタC1133に読み込まれた平文ブロックは、すべて独立であり、かつ、同じ暗号変換処理を行ことになる。したがって、CPU内の制御部1141が、レジスタAの暗号変換処理に実行部A1111を割当てて、レジスタBの暗号変換処理に実行部B1111を割当てて、レジスタCの暗号変換処理に実行部C1111を割当る。これによって、レジスタA1131とレジスタB1132とレジスタC1133の処理を、3本のパイプラインを用いて並列実行することができる。暗号変換処理が終了すると、それぞれのレジスタの値を、データ領域135の同じ場所に書きこみ、先頭の暗号文ブロックが生成される。これを、以降の平文ブロックに対しても、行っていくことで、平文フレームA221と、平文フレームB222と、平文フレームC223を、暗号文フレームA231と、暗号文フレームB232と、暗号文フレームC233に、並列に、暗号変換していく。同様な処理を、他の平文フレームでも行っていくことで、平文データ220の暗号変換を、並列処理することができる。

【0063】次に、暗号／復号変換システム1101が、具体的にはCPU1110が制御プログラムを実行し、暗号文データを復号変換する手順を図13を用いて説明してい

く。前述の実施例の復号変換システム801と同様に、暗号文データ230は、データ領域135に書き込まれていき、復号変換を行うために、フレームに分割され、さらに各フレームは、ブロックに分割される。図13においては、暗号文フレームA231が、暗号文ブロックC[1]251から暗号文ブロックC[n]258に分割される。

【0064】まず、レジスタA1131は、初期値領域から、初期値を読み込み、続いて、データ領域135から暗号文ブロックC[1]251を読み込みこむ。次にレジスタB1132は、データ領域135から、暗号文ブロックC[2]252と、暗号文ブロックC[2]251を読み込む。次に、レジスタC1133は、データ領域135から、暗号文ブロックC[3]253と、暗号文ブロックC[2]252を読み込む。レジスタA1131およびレジスタB1132およびレジスタC1133の処理は、すべて独立であるので、CPU内の制御部1141が、レジスタAの暗号変換処理に実行部A1111を割当てて、レジスタBの暗号変換処理に実行部B1111を割当てて、レジスタCの暗号変換処理に実行部C1111を割当る。これによって、レジスタA1131とレジスタB1132とレジスタC1133の処理を、3本のパイプラインを用いて並列実行することができる。暗号変換処理が終了すると、それぞれのレジスタの値を、データ領域135に書きこんでいく。レジスタA1131からは、平文ブロックM[1]が得られ、レジスタB1132からは、平文ブロックM[2]が得られ、レジスタC1133からは、平文ブロックM[3]が得られる。

【0065】同様な処理を、以降の暗号文ブロックについても行っていくことで、暗号文フレーム231の復号変換を、並列処理することができる。さらに、他の暗号文フレームに対しても、同様な処理を行うことで、暗号文データ230を並列に平文データ220に変換できる。

【0066】次に、暗号／復号変換システム1101が、並列に暗号／復号変換を行うための、メモリ1115のプログラム領域1181に格納される、制御プログラムの構成について、説明していく。

【0067】図14は、暗号変換の制御を行う暗号変換プログラム1203、および復号変換の制御を行う復号変換プログラム1213の生成手順を表している。暗号変換プログラム1203、および復号変換プログラム1213は、機械語であるので、暗号変換プログラム1203を生成するには、プログラム言語で書かれた、ソースコード1201を、コンパイラ1202でコンパイルする。同様に、復号変換1213を生成するには、ソースコード1211を、コンパイラ1202でコンパイルする必要がある。

【0068】次に、並列に暗号変換を行うためのソースコード1201の構成を説明する。まず、並列に暗号変換を行わない、通常の処理手順を記述した、ソースコードを図15に示す。前述したように、暗号変換はフレーム毎に行われる。それぞれのフレームの暗号変換処理は、複数の処理手順に分割されるが、それぞれの処理手順は、

1 5において、処理A 1 (1311)、処理A 2 (1312)、処理A 3 (1313)、...は、フレームAの暗号変換処理を表している。また、処理B 1 (1321)、処理B 2 (1322)、処理B 3 (1323)、...は、フレームBの暗号変換処理を表している。また、処理C 1 (1311)、処理C 2 (1312)、処理C 3 (1313)、...は、フレームCの暗号変換処理を表している。図13のソースコードのように、まず、フレームAを処理し、次にフレームBを処理し、次にフレームCを処理し、...というように、処理を記述していくと、全体の暗号変換処理は、並列化されない。次に、並列に暗号変換を行うように記述された、ソースコードを図16に示す。図16のソースコードは、まず、フレームAの処理A 1 (1311)と、フレームBの処理B 1 (1321)と、フレームCの処理C 1 (1331)を実行し、次に、フレームAの処理A 2 (1312)と、フレームBの処理B 2 (1322)と、フレームCの処理C 2 (1332)を実行し、次に、フレームAの処理A 3 (1313)と、フレームBの処理B 3 (1323)と、フレームCの処理C 3 (1333)を実行し、...というように、記述されている。このように記述すると、処理A 1 (1311)と、処理B 1 (1321)と、処理C 1 (1331)は独立であるので、並列に実行され、処理A 2 (1312)と、処理B 2 (1322)と、処理C 2 (1332)は独立であるので、並列に実行され、...というように、暗号変換を並列に処理していくことが可能になる。

【0069】次に、並列に復号変換を行うためのソースコード1211の構成を説明する。まず、並列に復号変換を行わない、通常の処理手順を記述した、ソースコードを図17に示す。前述したように、復号変換はブロック毎に行われる。それぞれのブロックの復号変換処理は、複数の処理手順に分割されるが、それぞれの処理手順は、1 5において、処理a 1 (1511)、処理a 2 (1512)、処理a 3 (1513)、...は、ブロックaの復号変換処理を表している。また、処理b 1 (1521)、処理b 2 (1522)、処理b 3 (1523)、...は、ブロックbの復号変換処理を表している。また、処理c 1 (1511)、処理c 2 (1512)、処理c 3 (1513)、...は、ブロックcの復号変換処理を表している。図17のソースコードのように、まず、ブロックaを処理し、次にブロックbを処理し、次にブロックcを処理し、...というように、処理を記述していくと、全体の復号変換処理は、並列化されない。次に、並列に復号変換を行うように記述された、ソースコードを図18に示す。図18のソースコードは、まず、ブロックaの処理a 1 (1511)と、ブロックbの処理b 1 (1521)と、ブロックcの処理c 1 (1531)を実行し、次に、ブロックaの処理a 2 (1512)と、ブロックbの処理b 2 (1522)と、ブロックcの処理c 2 (1532)を実行し、次に、ブロックaの処理a 3 (1513)と、ブロックbの処理b 3 (1523)と、ブロックcの処理c 3 (1533)を実行し、...とい

うように、記述されている。このように記述すると、処理a 1 (1511)と、処理b 1 (1521)と、処理c 1 (1531)は独立であるので、並列に実行され、処理a 2 (1512)と、処理b 2 (1522)と、処理c 2 (1532)は独立であるので、並列に実行され、...というように、復号変換を並列に処理していくことが可能になる。

【0070】上述した、実施形態の説明において、暗号／復号変換システム1001による、暗号および復号変換は、CBCモードを用いていたが、他の暗号運用モードを用いることも可能である。例えば、ブロック暗号方式をそのまま適用する基本モードである、ECB (Electronic Code Book) モードを用いる場合を考える。この場合、各フレーム内の各ブロックは、独立に処理することができるので、一つのフレームから、ブロックを複数個取り出し、取り出したそれぞれのブロックを、CPU 101内の別々の実行部で、同時に変換していく、ということを繰り返していくことで、並列処理を行うことができる。

【0071】次に、本発明の他の実施形態として、DVD (Digital Video Disc) などのパッケージコンテンツを流通させるシステムの実施例を図19に示す。

【0072】コンテンツプロバイダー1401は、著作権管理機関1418に著作権情報を登録し、コンテンツID情報IDA 1402を得る。IDAはデジタルデータにID情報などを隠しもたせる技術である電子透かしを用いてコンテンツデータ1403に埋め込まれ、パッケージコンテンツ1404となる。ここで、図20はパッケージコンテンツ1404内のコンテンツデータを表しており、コンテンツ情報IDA 1402が電子透かしとして含まれている。

【0073】情報家電B 1405がパッケージコンテンツ1404内のコンテンツデータをパーソナルコンピュータC 1411に転送する場合、情報家電B 1405は著作権管理機関1419から発行されたユーザID情報IDB 1407を電子透かしとしてコンテンツデータ内に埋め込み、本発明を用いた暗号装置1406で鍵データK 1408により暗号化し、外部バス上に暗号データを流す。図21は経路1409を流れるコンテンツデータを表しており、コンテンツ情報IDA 1402およびユーザID情報IDB 1407が電子透かしとして含まれている。

【0074】受信側であるパーソナルコンピュータC 1411は、暗号データを、本発明を用いた復号装置1413で鍵データK 1415により復号化する。以上の処理において、ユーザ情報や鍵データの管理にICカード1410を用いてもよい。

【0075】パーソナルコンピュータC 1411がネットワーク上にコンテンツデータを流通させる場合、パーソナルコンピュータC 1411は著作権管理機関1419から発行されたユーザID情報IDC 1414を電子透かしとしてコンテンツデータ内に埋め込み、本発明を用いた暗号装置1410で、データを鍵データK 1415により暗号化する。

図22は経路1409を流れるコンテンツデータを表しており、コンテンツ情報IDA 1402、ユーザID情報IDB 1407およびユーザID情報IDC 1414が電子透かしとして含まれている。以上の処理において、ユーザ情報や鍵データの管理にICカード1417を用いてもよい。

【0076】著作権管理機1419は、検査装置1419を用いて、ネットワーク上を流れるデータを監視し、暗号化されていないデータを検出した場合、データ内のコンテンツID情報を著作権情報管理データベース1420と照合し、不正コピーと判断すれば、不正コピーの発生場所をユーザID情報から追跡し、ペナルティを課す。

【0077】また、本発明を用いたデジタル衛星放送などのデジタルコンテンツの流通システムの実施例を図23に示す。コンテンツプロバイダー1401は、著作権管理機関1418に著作権情報を登録し、コンテンツID情報IDA

1402を得る。IDAを電子透かしとして埋め込んだコンテンツデータ1403は、放送センタ1801に送られ、既存の暗号装置1802で暗号化され、デジタル衛星放送受信機などの情報家電に向けて放送される。情報家電は既存の復号化装置1803で放送データを復号化する。情報家電には、既存の復号装置1803に加えて本発明を用いた暗号装置1406を備えており、その後のコンテンツデータの流通過程は図19における例と同様に行うことができる。

【0078】このように、デジタル衛星放送などの既存の暗号システムと本発明の暗号システムを組み合わせ、デジタルコンテンツの流通システムを構築することも可能であり、パッケージメディア、放送メディア、通信メディアと幅広く本発明の適用が可能である。

【0079】

【発明の効果】本発明によれば、データの暗号変換を、または復号変換をそれぞれ高速に処理することができる。

【図面の簡単な説明】

【図1】本発明を用いた、情報処理機器の第1実施例である。

【図2】第1実施例における、暗号変換手順の詳細図である。

【図3】第1実施例における、復号変換手順の詳細図である。

【図4】図1における、変換部の詳細図である。

【図5】図1における、情報処理機器が、暗号変換と、復号変換を同時に行う場合の概要図である。

【図6】図1における、暗号／復号変換システムで、複数のデータを、リアルタイムに、暗号／復号変換するために用いる管理情報の詳細図である。

【図7】図1における、暗号／復号変換システムで、複数のデータを、リアルタイムに、暗号／復号変換するための、管理手順のフローチャートである。

【図8】本発明を用いた、情報処理機器の他の実施例で*

*ある。

【図9】他の実施例における、復号変換手順の詳細図である。

【図10】図8における、変換部の詳細図である。

【図11】本発明を用いた、情報処理機器の他の実施例である。

【図12】他の実施例における、暗号変換手順の詳細図である。

【図13】他の実施例における、復号変換手順の詳細図である。

【図14】制御プログラムの、生成手順の概要図である。

【図15】暗号変換を行うように記述された、ソースコードの概念図(その1)である。

【図16】暗号変換を行うように記述された、ソースコードの概念図(その2)である。

【図17】復号変換を行うように記述された、ソースコードの概念図(その1)である。

【図18】復号変換を行うように記述された、ソースコードの概念図(その2)である。

【図19】本発明を用いたパッケージコンテンツの流通システムに関する一実施例である。

【図20】電子透かしを含むコンテンツデータ(その1)である。

【図21】電子透かしを含むコンテンツデータ(その2)である。

【図22】電子透かしを含むコンテンツデータ(その3)である。

【図23】本発明を用いた放送コンテンツの流通システムに関する一実施例である。

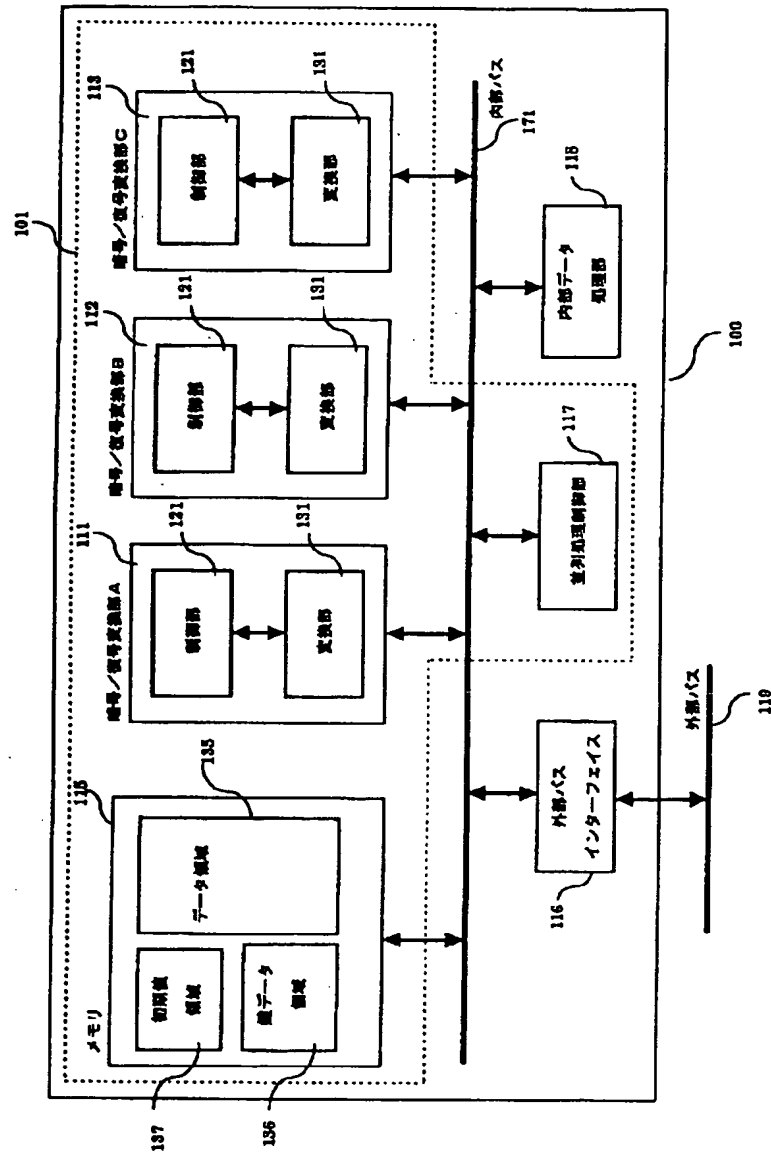
【図24】CBCモードによる、暗号変換および復号変換の処理手順の詳細図である。

【符号の説明】

- 100…情報処理機器、
- 101…暗号／復号変換システム、
- 111…暗号／復号変換部A、
- 112…暗号／復号変換部B、
- 113…暗号／復号変換部C、
- 115…メモリ、
- 116…外部バスインターフェイス、
- 117…並列処理制御部、
- 118…内部データ処理部、
- 119…外部バス、
- 121…制御部、
- 131…変換部、
- 135…データ領域、
- 136…鍵データ領域、
- 137…初期値領域、
- 171…内部バス。

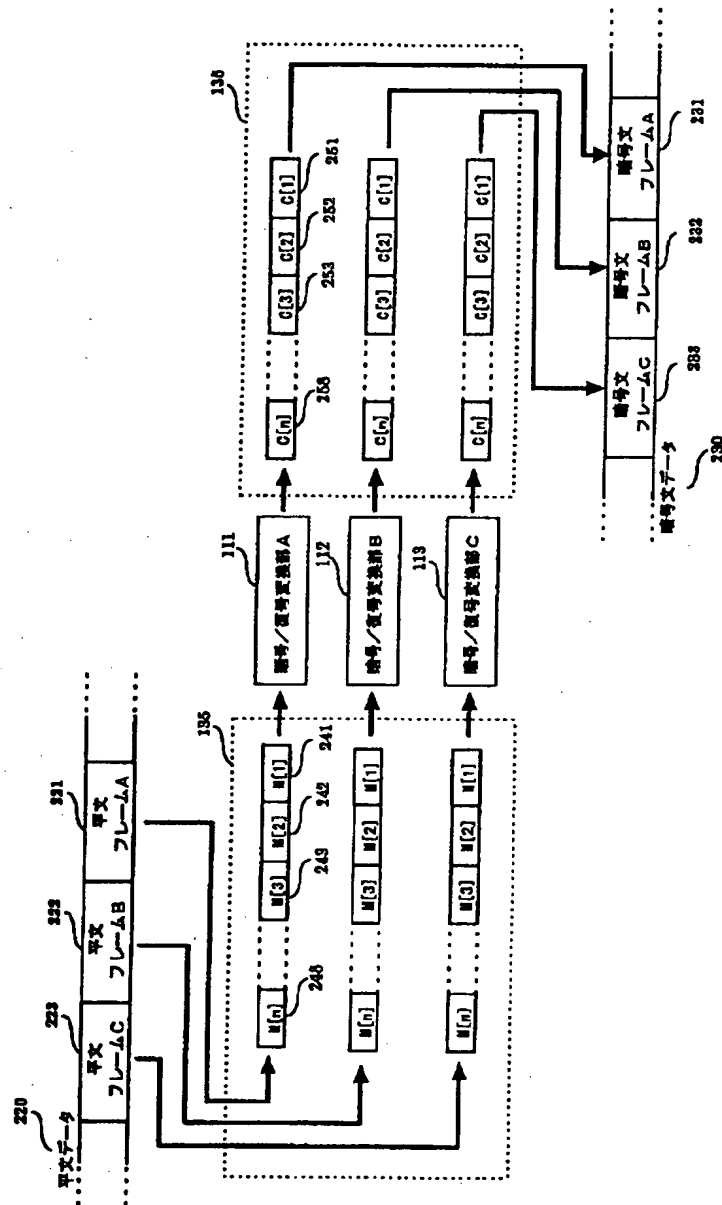
【図1】

図 1



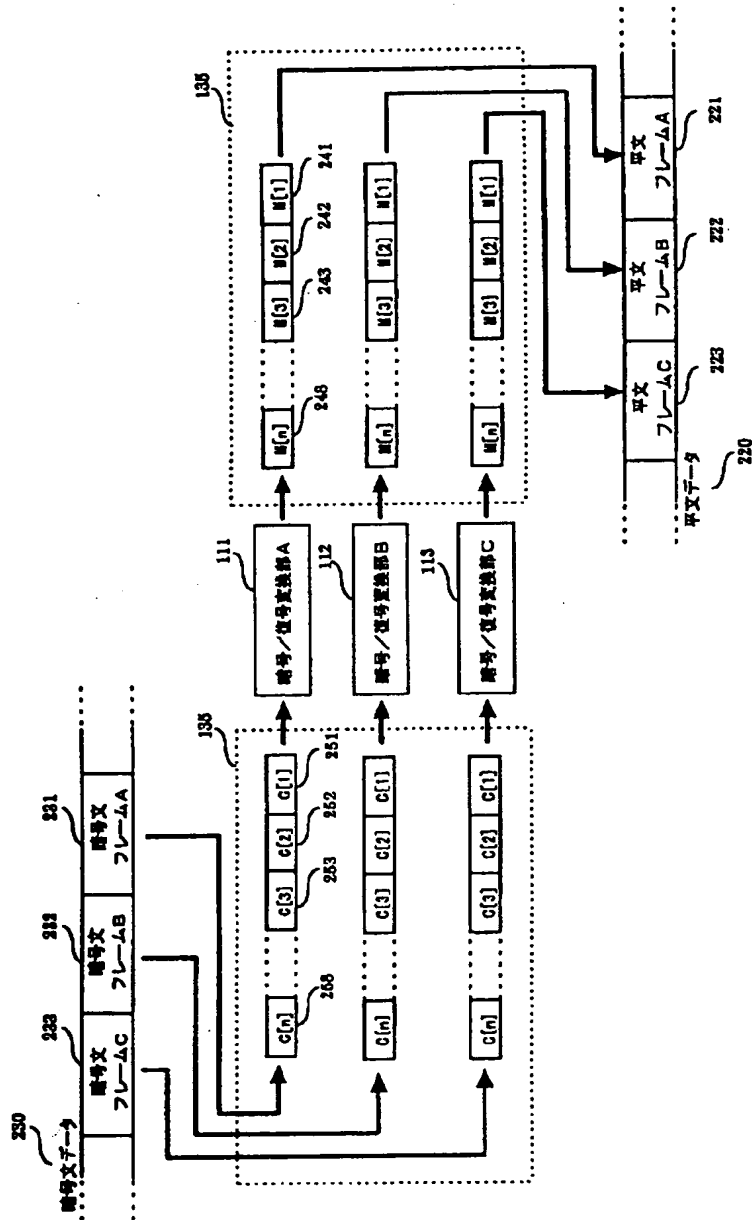
【図2】

図 2



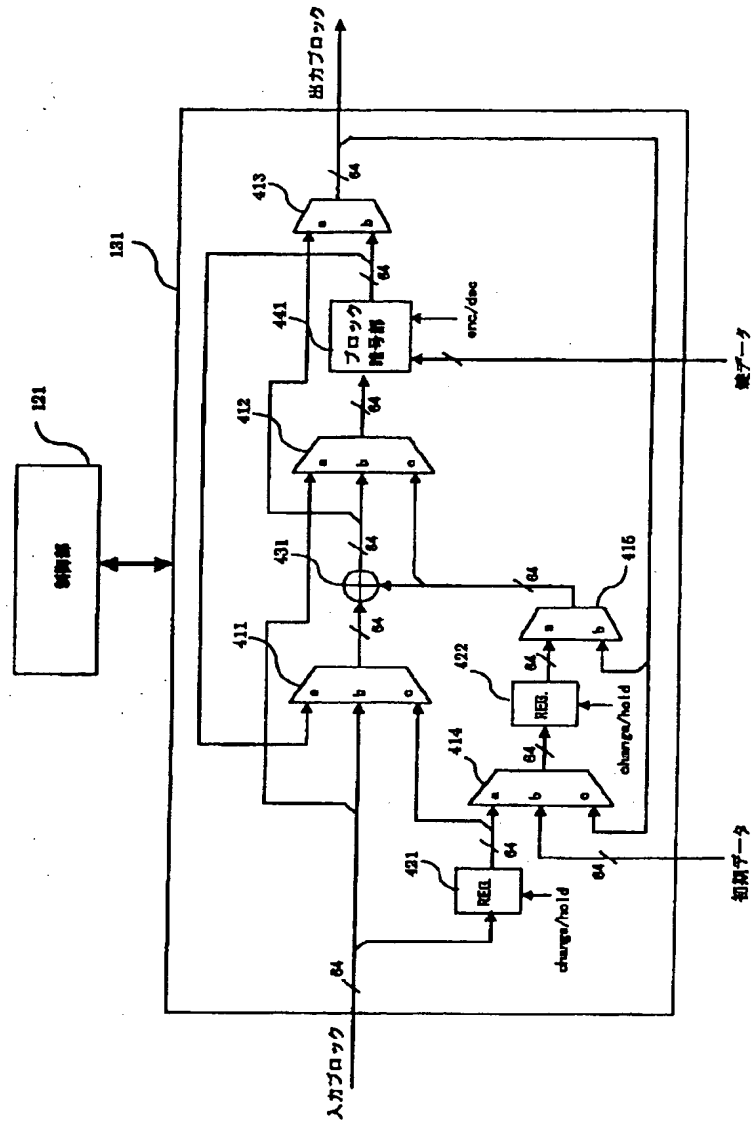
【図3】

図 3



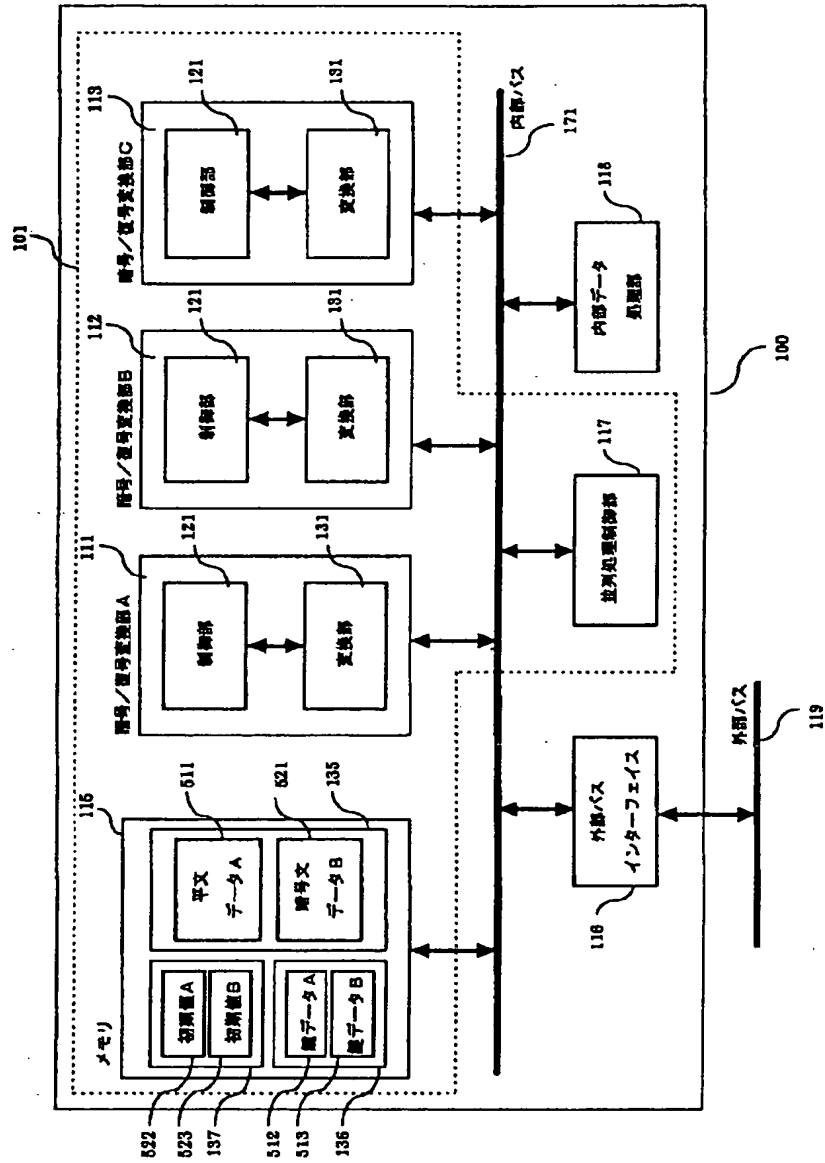
【図 4】

4



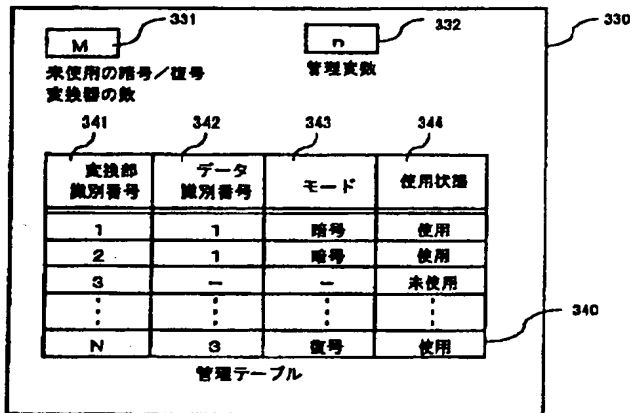
【図5】

図 5



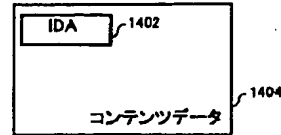
【図6】

図 6



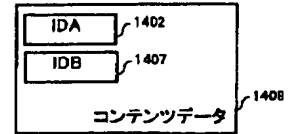
【図20】

図 20



【図21】

図 21



【図10】

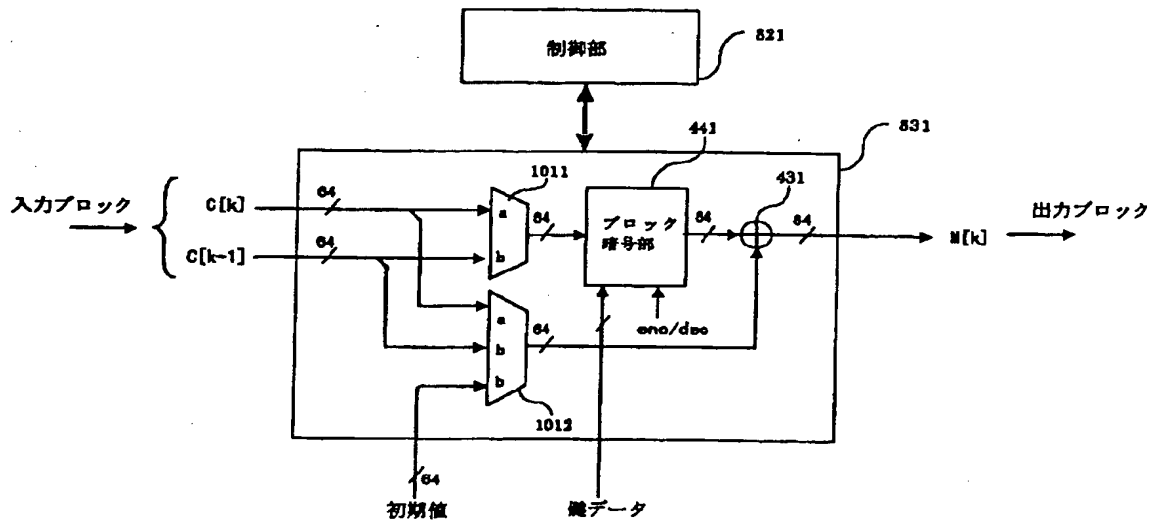
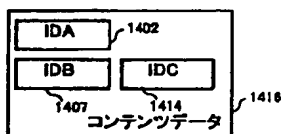


図 10

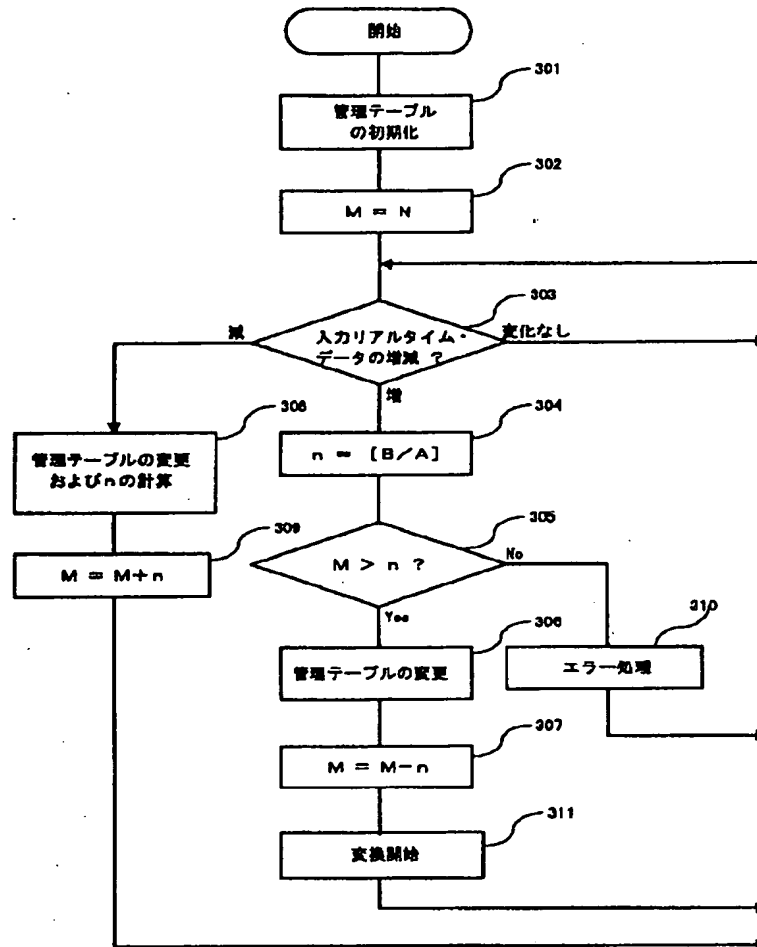
【図22】

図 22



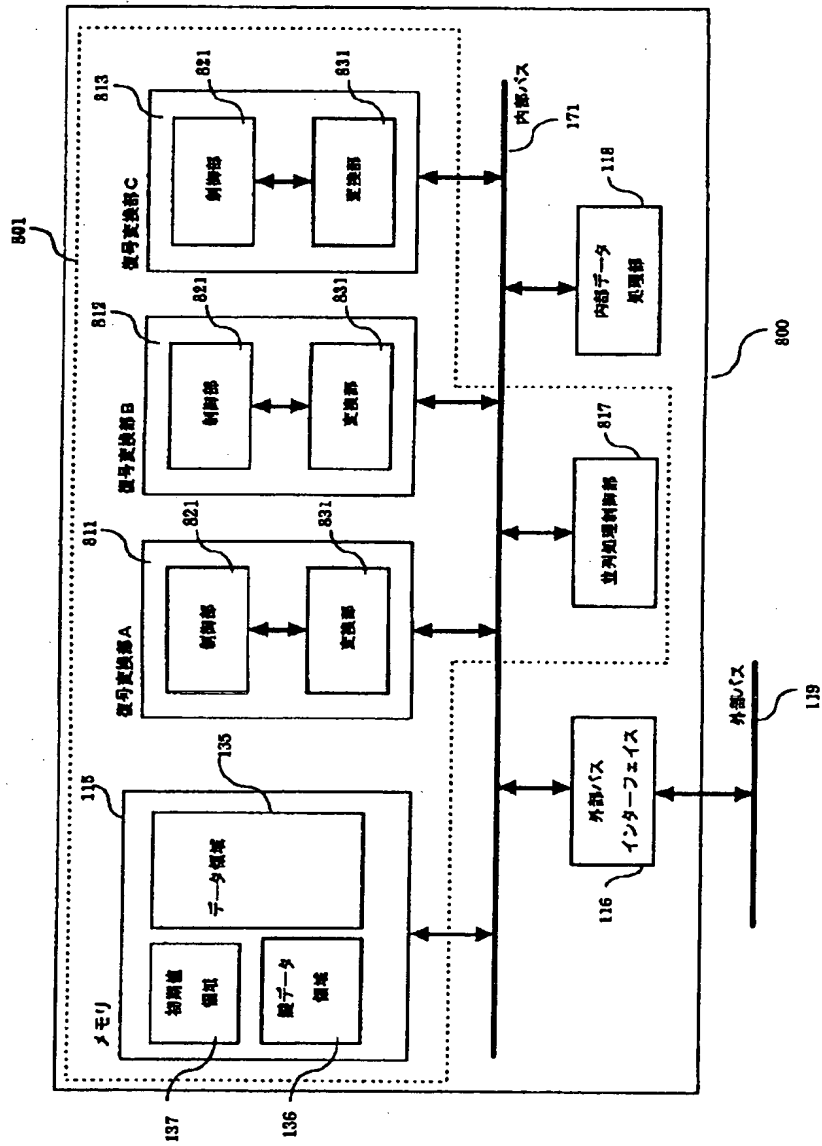
【図 7】

図 7



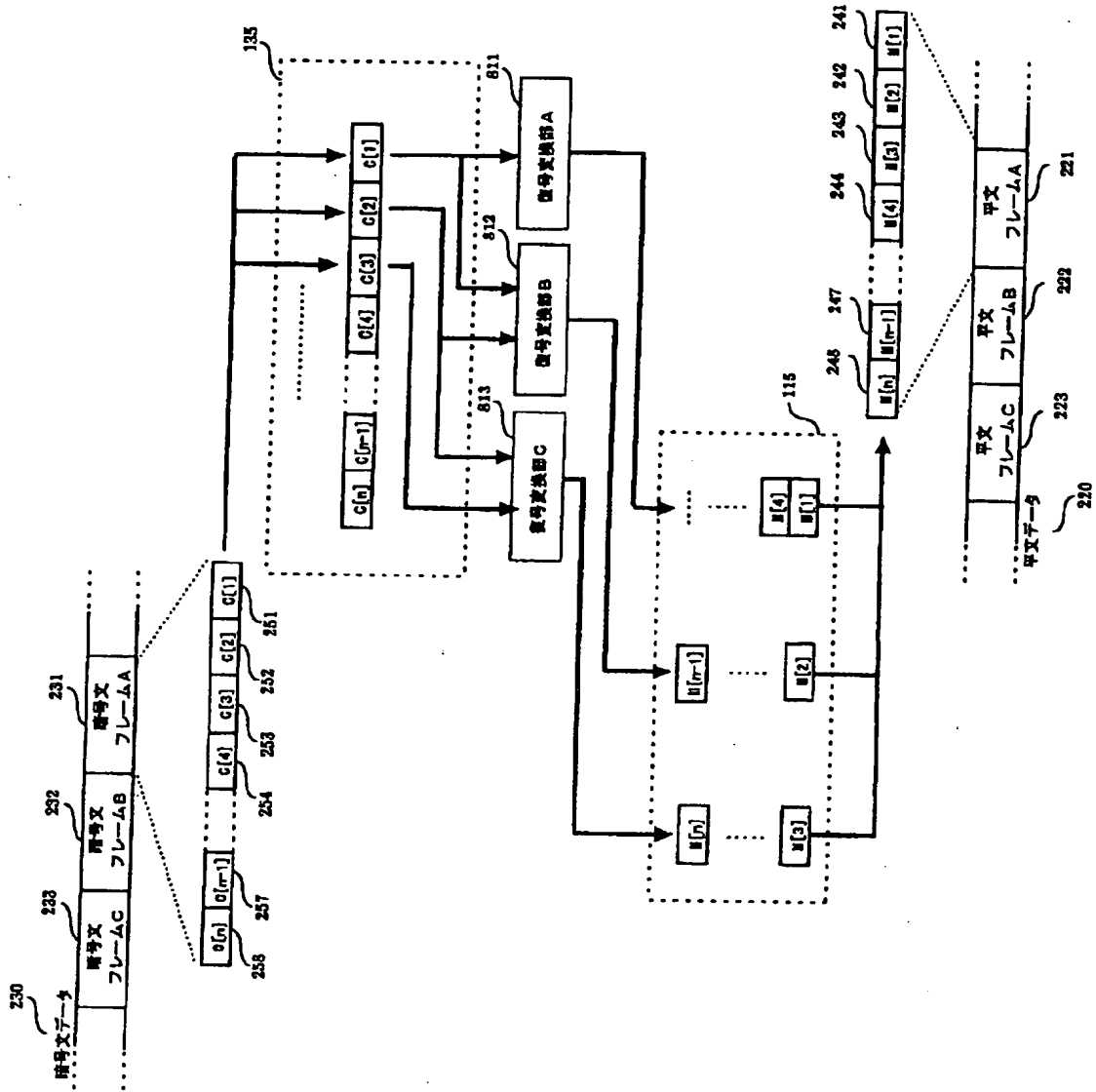
【図8】

図 8



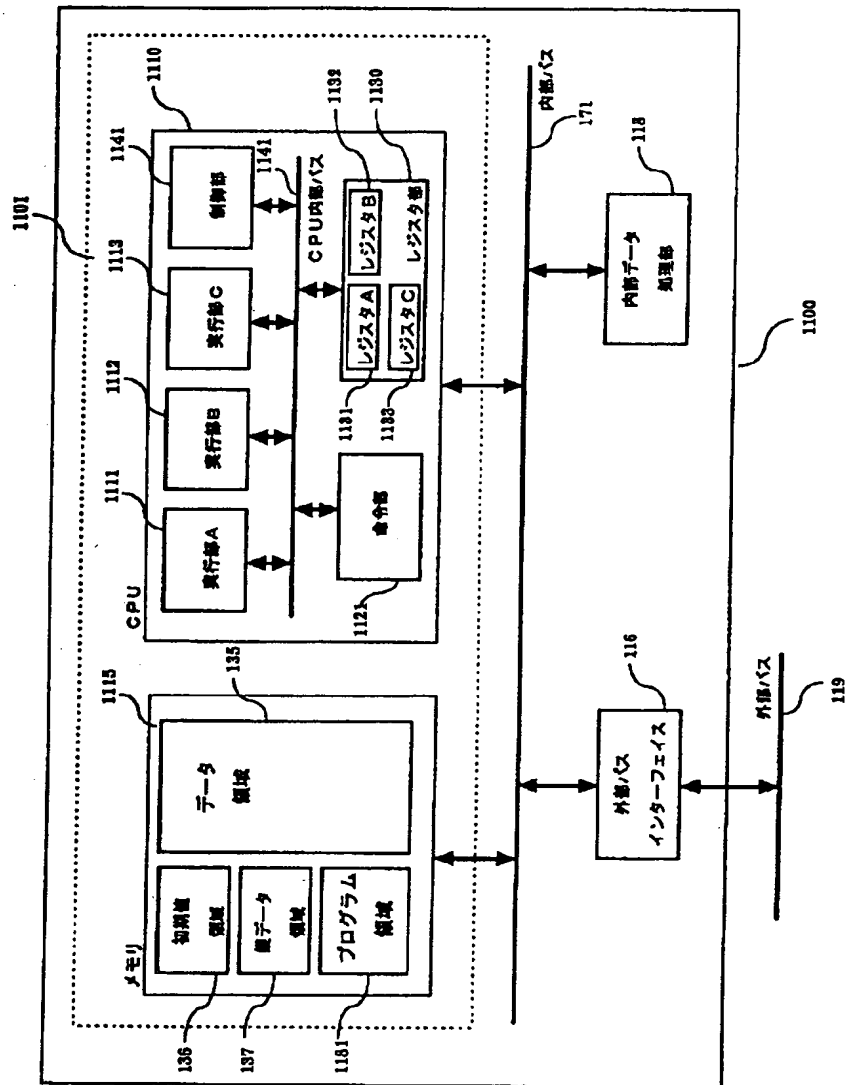
【図 9】

図 9



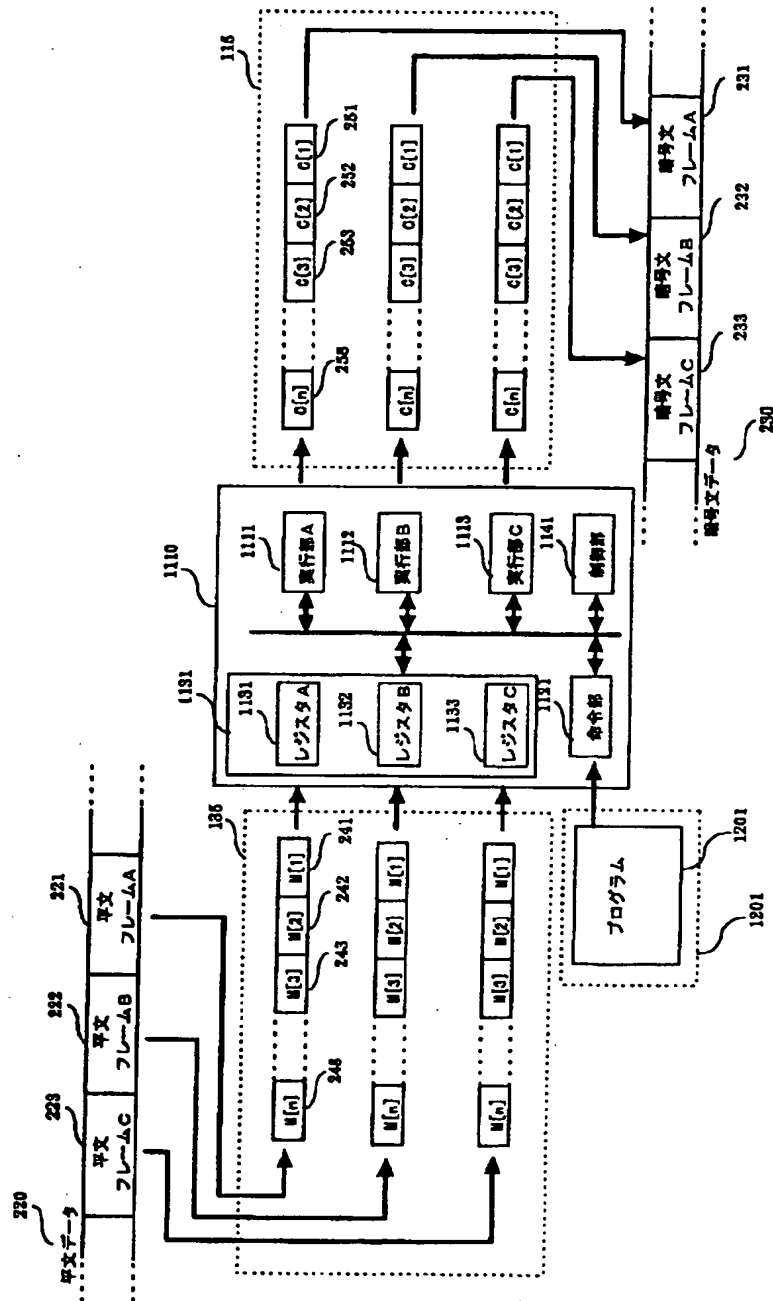
【図 11】

図 11

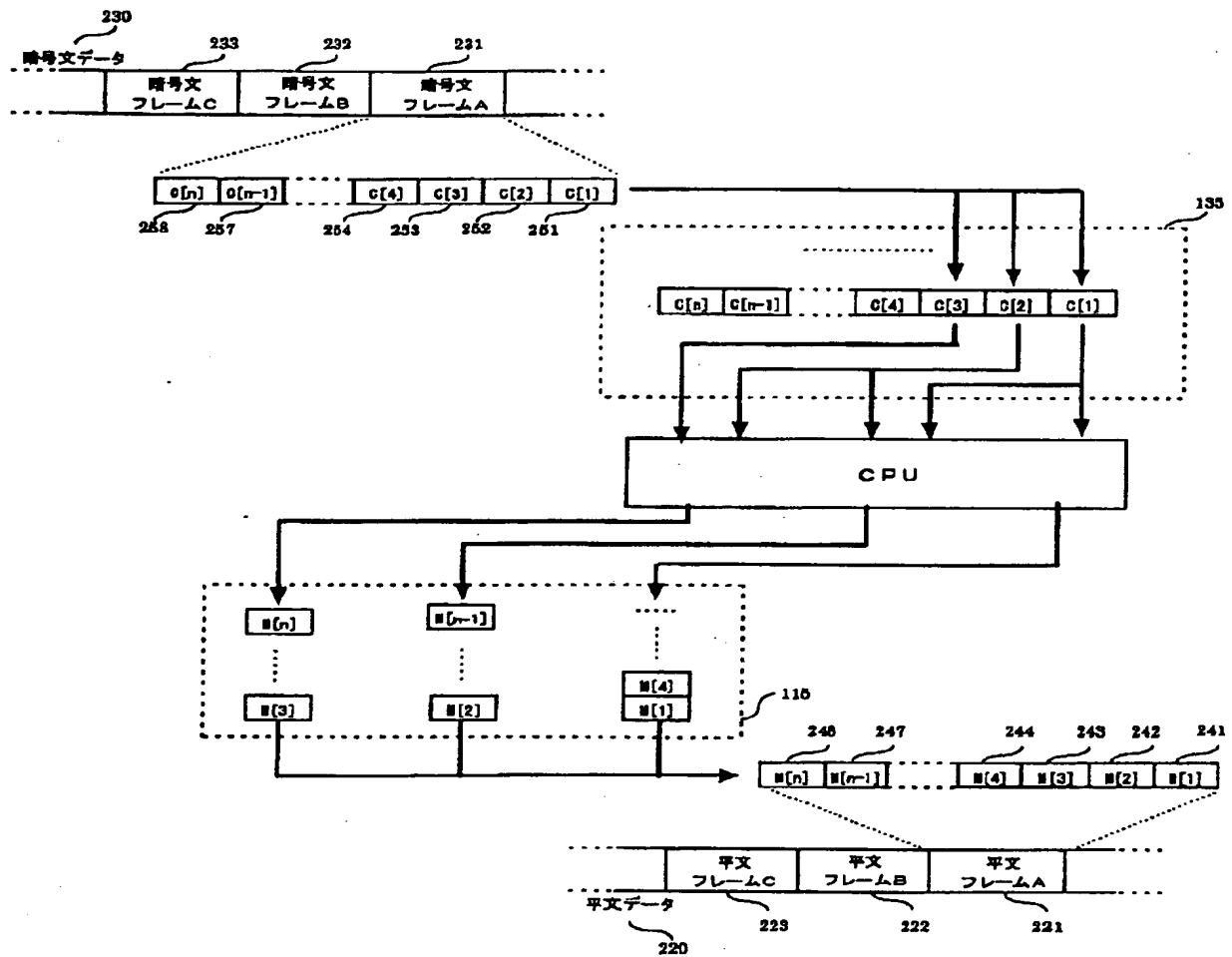


【図12】

図 12

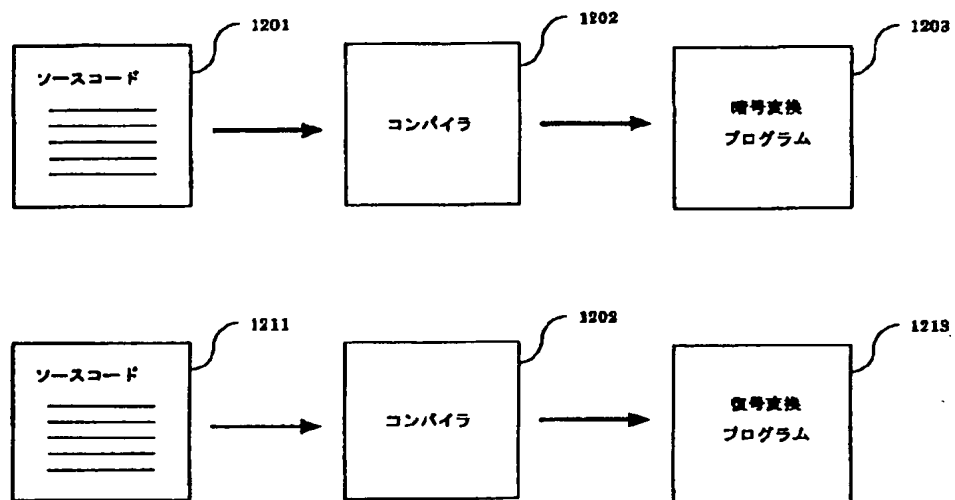


【図13】



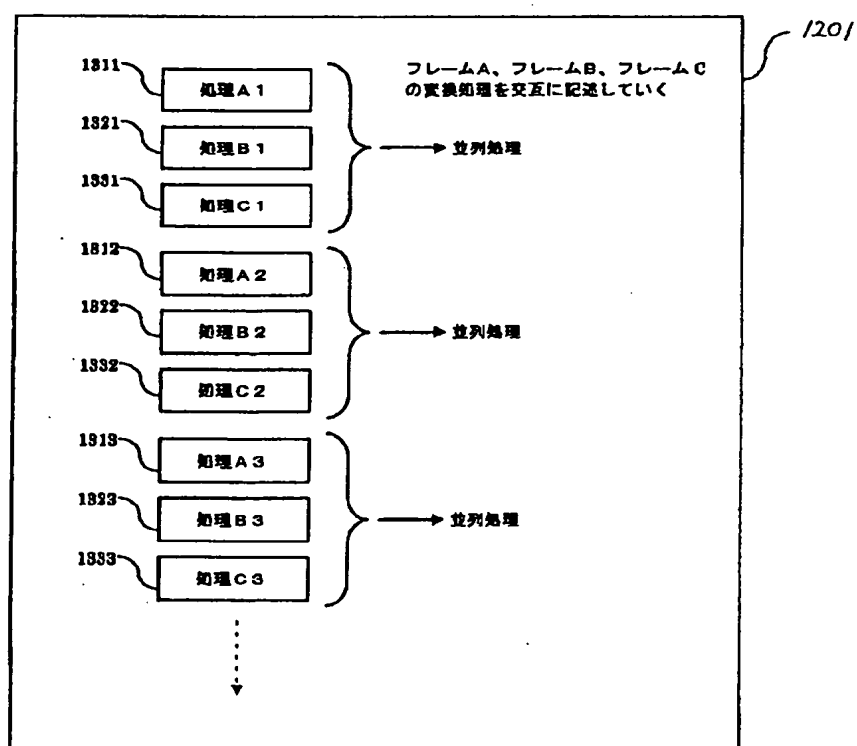
【図 14】

図 14



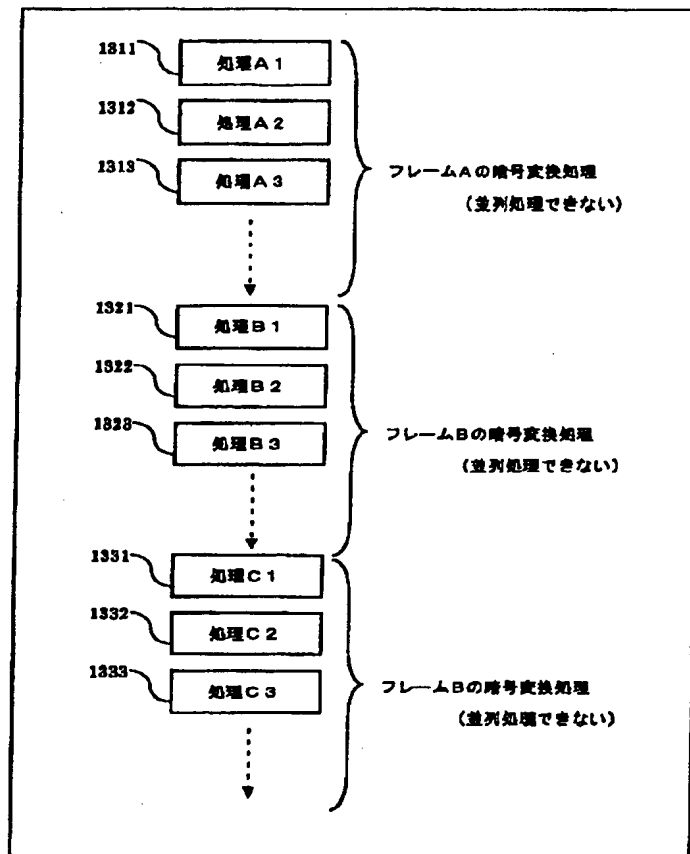
【図 16】

図 16



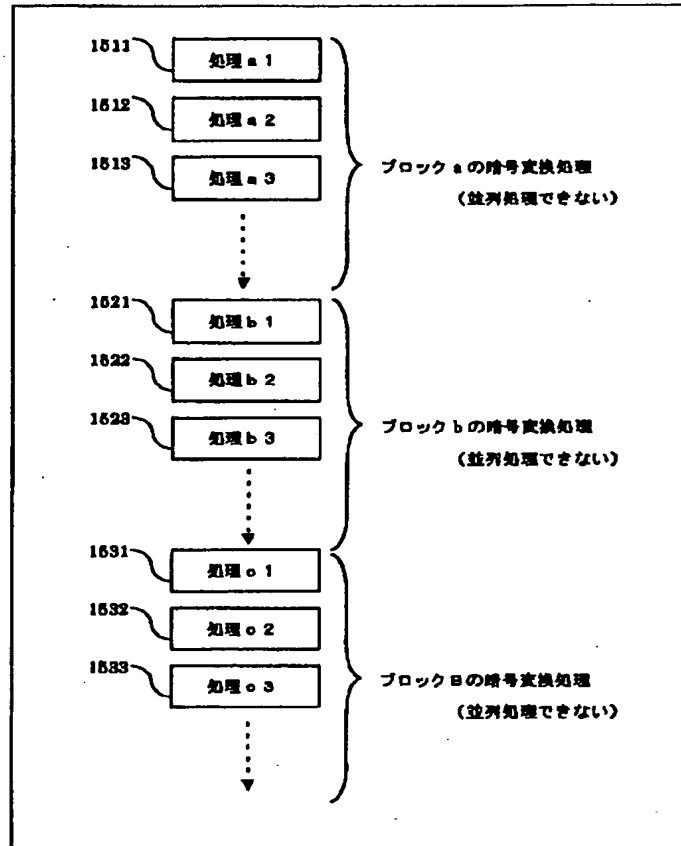
【図15】

図 15



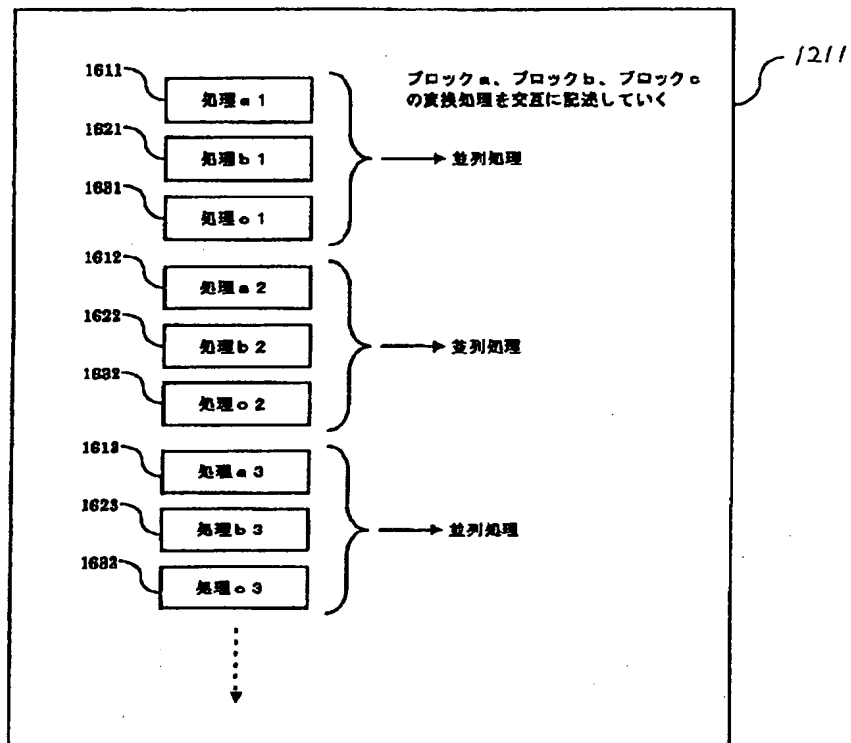
【図 17】

図 17



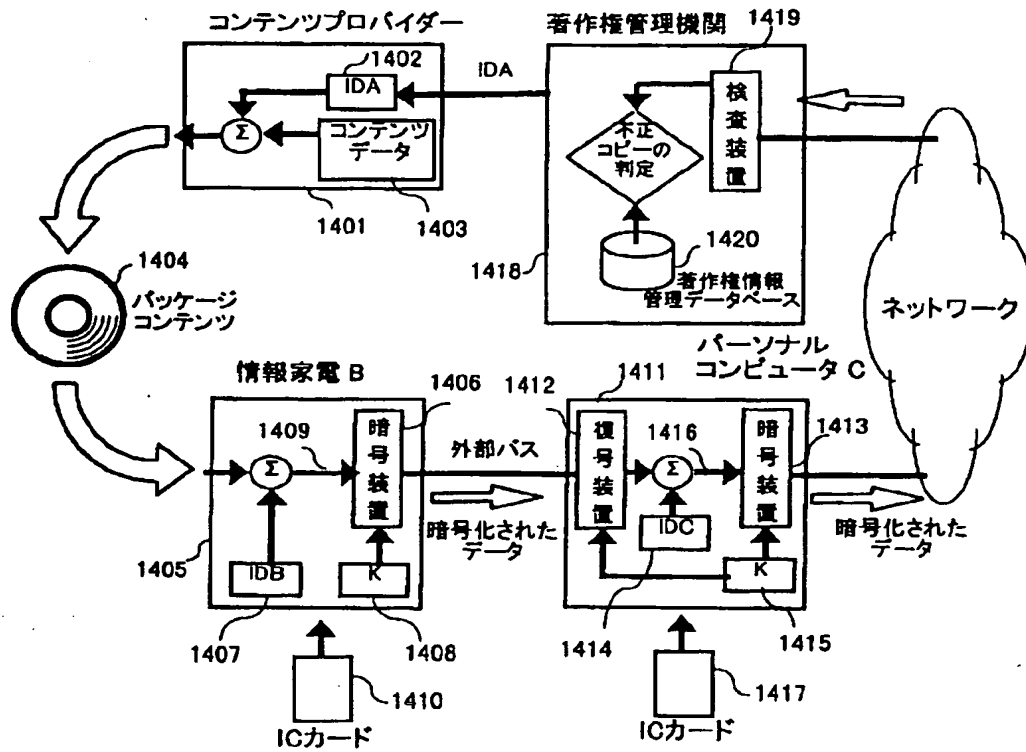
【図 18】

図 18



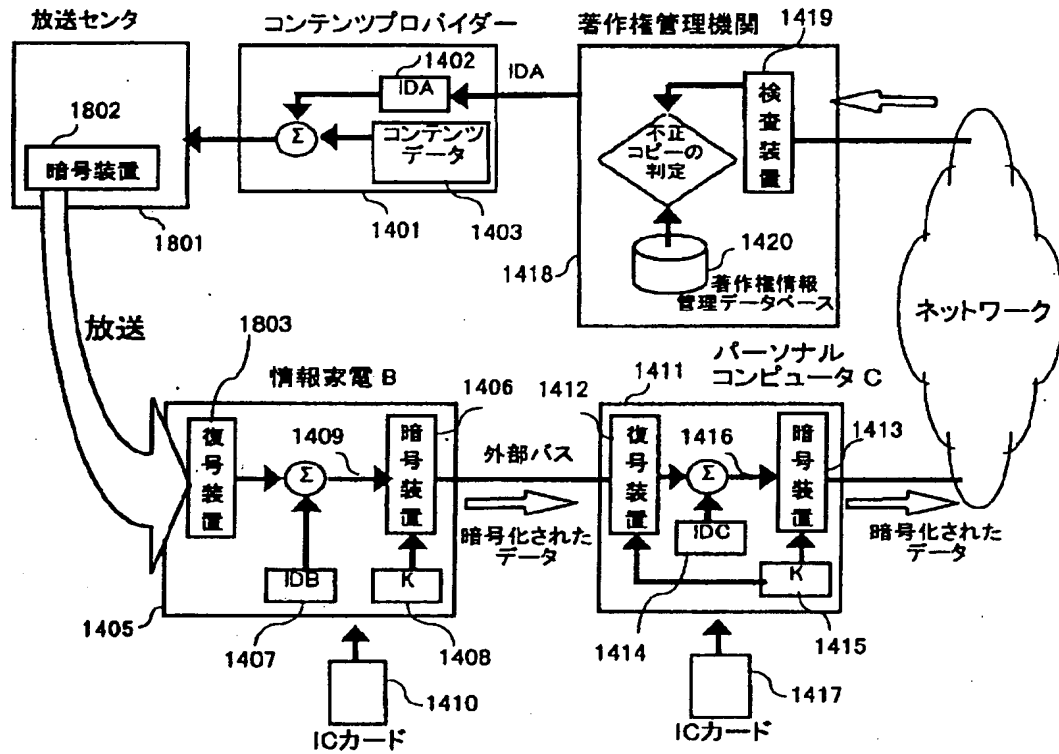
【図 19】

図 19



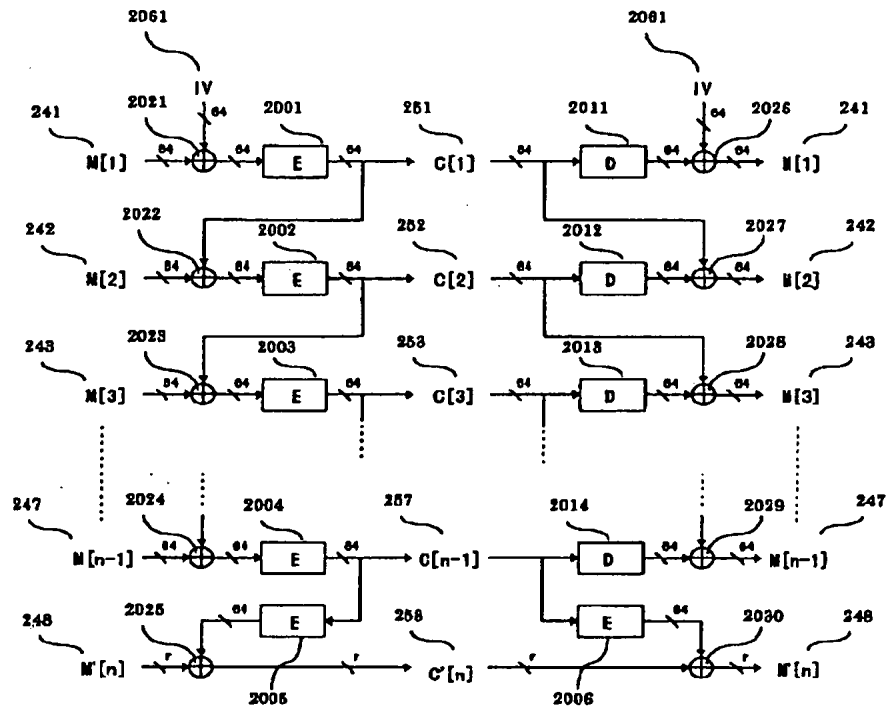
【図23】

図 23



【図24】

図 24



フロントページの続き

(72)発明者 古屋 聡一
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 平島 茂
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所マルチメディアシステム
開発本部内

THIS PAGE BLANK (USPTO)